RMIT UNIVERSITY

Reliable and Secure Low Energy Sensed Spectrum Communication for Time Critical Cloud Computing Applications

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

Uthpala Subodhani Premarathne

BTech.Hons.(NITW), MSc(Moratuwa)

School of Science

College of Science, Engineering and Health

RMIT University

October, 2017

Declaration

I certify that except where due acknowledgment has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; and, any editorial work, paid or unpaid, carried out by a third party is acknowledged.

U S Premarathne
School of Computer Science and Information Technology
RMIT University

Acknowledgments

First and foremost, I would like to thank my supervisors, Dr. Ibrahim Khalil and Professor Zahir Tari. I greatly appreciate all the support, guidance, and encouragement provided to make my PhD experience productive and stimulating. Sincere thanks go to Professor Mohammed Atiquzzaman, University of Oklahoma and Professor Bharat Bhargave, Purdue University for their support and guidance. Gratefully acknowledge the funding sources: both RMIT University and the National ICT Australia (NICTA), for the financial support for the four years of my PhD research. I wish to thank my fellow PhD students, the academic and academic support staff members of School of Computer Science and IT, RMIT University for their companionship and collegiality. Sincere thanks goes to Melanie for proof reading the entire thesis and for her constructive feedback. Gratefully acknowledge the inputs, suggestions and all the support extended by colleagues at the Department of Computational Mathematics and the Department of Electronics and Telecommunications Engineering at the University of Moratuwa to complete the thesis revision.

I am so grateful for my family for all their love and encouragement. My beloved children, Megha putha and Miyasi duwa light up my life always. Sincere thanks go to my husband, Upeka Kanchana Premaratne, for all his encouragement extended throughout the years. I am grateful to my parents for raising me with a passion for learning and supporting me in all my pursuits. Without the unconditional love, support and constant encouragement from my mother, I would not have come this far. I am so grateful for my uncle Dr. Uditha Balasooriya, my grandfather and grandmother for extending strong emotional support during the tough times with their continuous blessings to succeed. Finally, I thank all my relatives and friends for extending their love and support over the years in numerous ways.

Credits

Portions of the material in this thesis have previously appeared in the following publications:

- [Premarathne et al. 2016] U. S. Premarathne, I. Khalil and Mohammed Atiquzzaman, "Trust based Reliable Transmission Strategies for Smart Home Energy Management in Cognitive Radio based Smart Grid", Ad hoc Networks (*Impact Factor:1.53*): Special Issue on Cognitive Radio Based Smart Grid: The Future of the Traditional Electrical Grid, vol. 41, pp. 15-29, 2016. (**Chapter 3**)

- U.S. Premarathne and I. Khalil, "Reliable Delay Sensitive Re-Entrant Sensed Spectrum Transmission", The manuscript is being reviewed in Adhoc Networks, Elsevier. (**Chapter 4**).

- [Premarathne et al. 2015c] U. S. Premarathne, I. Khalil and M. Atiquzzaman," Secure and Reliable Surveillance over Cognitive Radio Sensor Networks in Smart Grid", Pervasive and Mobile Computing (*Impact Factor:2.079*): Special Issue on Recent Developments in Cognitive Radio Sensor Networks, vol.22, pp.3-15, September 2015. (**Chapter 5**)

- [Premarathne et al. 2015a] U.S Premarathne, I. Khalil, Z. Tari and A. Zomaya," Cloud-based Utility Service Framework for Trust Negotiations using Federated Identity Management", IEEE Transactions on Cloud Computing, vol.5, no.2, pp.290-302, 2015. (**Chapter 6**)

- [Tari et al. 2015] Z. Tari, X. Yi, U.S Premarathne, P. Bertok and I. Khalil," Security and Privacy in Cloud Computing: Vision, Trends, and Challenges", Cloud Computing, IEEE, vol.2, no.2, pp.30-38, 2015. (**Chapter 6**)

- [Premarathne et al. 2015b] U. S. Premarathne, I. Khalil and M. Atiquzzaman," Location dependent disclosure risk based decision support framework for persistent authentication in pervasive computing applications", Computer Networks (*Impact Factor:1.256*), vol.88, pp.161-177, 2015. (**Chapter 7**)

Contents

List of Figures

List of Tables

Nomenclature

Acronyms

TCRMS	Time Critical Remote Monitoring System
CR	Cognitive Radio
CRN	Cognitive Radio Network
CRSN	Cognitive Radio Sensor Network
PUF	Physically Unclonable Function
PU	Primary User
SU	Secondary User
FC	Fusion Center
SSDF	Spectrum Sensing Data Falsification
MADM	Multi-Attribute Trust Metric
IDP	Identity Provider
CSP	Cloud Service Provider
SP	Service Provider
LDDR	Location Dependent Disclosure Risk
PDCM	Policy Dependent Cost Metric
ISM	Industrial, Scientific and Medical
WLAN	Wireless Local Area Network
UMTS	Universal Mobile Telecommunication System
GSM	Global System of Mobile communication
GRPS	General Packet Radio Service
WiFi	Wireless Fidelity
ISO	International Standard Organization
MTTF	Mean Time To Failure
BS	British Standard
WSN	Wireless Sensor Networks

RF	Radio Frequency
RFID	Radio Frequency Identification
IDM	IDentity Management
ID	IDentity
TC	Trusted Coalition
KLD	Kullback-Leibler Divergence
NB	Naive Bayes
MP	Multi-layer Perceptron
TP	True Positive
FP	False Positive
IEEE	Institute of Electrical and Electronic Engineers
EDF	Earliest Deadline First
LLF	Least Laxity First
XOR	Exclusive-OR operation
SNEP	Sensor Network Encryption Protocol
TM	Throughput Metric
EECC	Energy Efficiency to support CR Communications
EESK	Energy Efficient Secure Key generation
AKCL	Adaptive encryption Key length selection to Control Leakages
SAMA	Security Against Masquerading Attacks
X-DoS	Extensible markup language - Denial of Service
DDoS	Distributed Denial of Service
OSDVB	Open Source Vulnerability Database
CVE	Common Vulnerabilities and Exposure
NVD	National Vulnerability Database
EDF	Earliest Deadline First
LLF	Least Laxity First
MLLF	Modified Least Laxity First

MUF	Maximum Urgency First
ALA	Application Log Analyses
AV	Anti-virus
CUM	Cache Usage Management
PF	Packet Filtering
PLA	Packet Level Analyses
MA	Message Analysis
ED-AL	Event Detection at Application Level
LM	Load Measurement
APUM	Automated Patch Update Mechanism
TF	Trust Framework
RBAC	Role Based Access Control
BTG	Break-the-glass
RBAC-A	RBAC variant with attribute based access control
ASL	Authorization Specification Language
LTL	Linear Temporal Logic
RV-LTL	Runtime Verification LTL

Operators and Functional Notations

$\|\cdot\|$	Absolute value of a scalar argument or determinant of a matrix
$\vee$	Binary maximum operator ($a \vee b = a$ when $a > b$)
$\wedge$	Binary minimum operator ($a \wedge b = b$ when $a > b$)
$\|, \bigvee$	Logical OR operator
$\&, \bigwedge$	Logical AND operator
$\cap$	Set intersection operator
$\cup$	Set union operator
$\sum$	Summation operator
$\prod$	Product operator
$\top$	truth value to express inconsistency as an over-knowledge
$\bot$	truth value to express inconsistency as no-knowledge
$\bigotimes$	Multiplicative conjuction
$\leftarrow$	Assignment operator
$E[]$	Mathematical Expectation

Abstract

Reliability and security of data transmission and access are of paramount importance to enhance the dependability of time critical remote monitoring systems (e.g. tele-monitoring patients, surveillance of smart grid components). Potential failures for data transmissions include wireless channel unavailability and delays due to the interruptions. Reliable data transmission demands seamless channel availability with minimum delays in spite of interruptions (e.g. fading, denial-of-service attacks). Secure data transmissions require sensed data to be transmitted over unreliable wireless channels with sufficient security using suitable encryption techniques. The transmitted data are stored in secure cloud repositories. Potential failures for data access include unsuccessful user authentications due to mis-management of digital identities and insufficient permissions to authorize situation-specific data access requests. Reliable and secure data access requires robust user authentication and context-dependent authorization to fulfill situation specific data utility needs in cloud repositories. The work herein seeks to enhance the dependability of time critical remote monitoring applications, by reducing these failure conditions which may degrade the reliability and security of data transmission or access.

As a result of an extensive literature survey, in order to achieve the above said security and reliability, the following areas have been selected for further investigations.

- The enhancement of opportunistic transmissions in cognitive radio networks to provide greater channel availability as opposed to fixed spectrum allocations in conventional wireless networks.

- Delay sensitive channel access methods to ensure seamless connectivity in spite of multiple interruptions in cognitive radio networks.

- Energy efficient encryption and route selection mechanisms to enhance both secure and reliable data transmissions.
- Trustworthy digital identity management in cloud platforms which can facilitate efficient user authentication to ensure reliable access to the sensed remote monitoring data.
- Context-aware authorizations to reliably handle the flexible situation specific data access requests.

Main contributions of this thesis include a novel trust metric to select non-malicious cooperative spectrum sensing users to reliably detect vacant channels, a reliable delay-sensitive cognitive radio spectrum hand-off management method for seamless connectivity and an energy-aware physical unclonable function based encryption key size selection method for secure data transmission. Furthermore, a trust based identity provider selection method for user authentications and a reliable context-aware situation specific authorization method are developed for more reliable and secure date access in cloud repositories. In conclusion, these contributions can holistically contribute to mitigate the above mentioned failure conditions to achieve the intended dependability of the time-critical remote monitoring applications.

CHAPTER 1

Introduction

Time-critical remote monitoring systems (TCRMSs) collect large volumes of data using sensors and data aggregators. By using the remote monitoring data, time-critical decisions are made. Examples of TCRMSs include, monitoring of critical components in the smart grid [Wang et al. 2013], telemonitoring applications in pervasive healthcare [Soomro and Cavalcanti 2007][Korhonen et al. 2003][Feng et al. 2010], remote status monitoring of propulsion systems [Horvitz 1995], building management systems [Suryadevara et al. 2015] and ambient assisted living home care solutions for the elderly [Kleinberger et al. 2009] [Botia et al. 2012][Bisio et al. 2015]. The dependability of TCRMSs rely on how efficiently these data are handled by minimizing the associated delays during transmission and access. For example, in TCRM applications on electric fire detection [Herald 2014] and propulsion system monitoring [Horvitz 1995], the main impediments for timely critical decision making include the failure of the communication infrastructure [Gungor et al. 2013] [Ma et al. 2013], the delays due to communication latency and rigorous access control.

In most of these emerging sensory arrangements of TCRMSs, wireless networks are used for data transmission [Akan et al. 2012] [Shah et al. 2013] [Maler and Reed 2008] [Suryadevara et al. 2015]. To realize sensed data transmission using a sufficiently secure encryption mechanism is a significant challenge in the resource constrained devices. In wireless networks, spectrum utilization is a delay-prone critical issue due to its highly

competitive nature [Mitola and Maguire 1999] [Haykin 2005] [Yin et al. 2012] [Tragos et al. 2013]. Even though the bandwidth may be reserved for different applications, it is often not regularly utilized to its full capacity. This is the motivation for cognitive radio networks, that sense the spectrum using intelligent transceivers and transmit data over the vacant channels [Akyildiz et al. 2006] [Haykin 2005]. Thus, the opportunistic spectrum utilization becomes an effective solution to reduce delays due to channel unavailability. In TCRMSs, data is accessed by the decision making agents for operations and maintenance requirements. Cloud computing infrastructure are increasingly used as scalable data storages and efficient distributed platforms to effectively manage the digital identities and rigorous access control [Buyya et al. 2010] [Zissis and Lekkas 2012] [Thilakanathan et al. 2014][Pandey et al. 2012] [Solanas et al. 2014] [Liang et al. 2012][Satyanarayanan et al. 2013].

Example Application - In a power generation remote monitoring system with cloud based data storage and access management (e.g. Netbiter [Netbiter 2017], Cummins solutions [Cummins 2017]), various data logs are accessed to make time critical decisions. A power generation remote monitoring system generates different sets of data, such as annunciator, alternator and engine data, transfer switch data, source, load and switch connection status data etc [Cummins 2017] and transmitted over wireless channels. The data are stored in secure cloud repositories. When there are number of distributed power generation plants, the secure cloud storages may be remotely accessed by the decision making agents from other locations.

A brief comparison of different techniques and devices that are used in different TCRMSs is shown in Table 1.1. In summary, almost all of the TCRMSs make use of different wireless technologies for data transmission. Majority of the TCRMSs use low power sensor nodes for data generation. In these light-weight sensors, a large proportion of energy is used for data transmission when compared to that of processing, encryption and computation [Gunduz et al. 2014] [Kinalis et al. 2014] [Tutuncuoglu and Yener 2012]. In most TCRM applications, the data is stored in cloud platforms to provide distributed access to the decision making agents.

Table 1.1: Summary of Different Data Generation, Transmission and Access Mechanisms for Different Time Critical Remote Monitoring (TCRM) Applications.

Application Categories	**Examples**
Electric system automation - C1	[Gungor and Lambert 2006] [Lu and Gungor 2009]
Surveillance applications (e.g. smart grid) - C2	[Wang et al. 2013] [Premarathne et al. 2015c] [Bicen et al. 2012a] [Li et al. 2012a] [Qiu et al. 2011]
Patient Health monitoring applications - C3	[Soomro and Cavalcanti 2007] [Korhonen et al. 2003] [Pantelopoulos and Bourbakis 2010] [Al Mamun et al. 2017] [Spanò et al. 2016] [Petäjäjärvi et al. 2016] [Immoreev and Ivashov 2008] [Shah et al. 2016]
Fire monitoring applications-C4	[Anghel et al. 2016] [Wang et al. 2016b]
Building monitoring applications - C5	[Dutta and Roy 2017] [Pacheco et al. 2016]
Devices/Technologies	**Examples**
Data Generation	sensors (C1,C2,C3,C4,C5), wireless sensor devices with larger memory (C1), wearable biosensors (C3)
Data Transmission	wireless sensor networks (C1,C2,C3,C5), optical fiber networks, Wireless Local Area Network (WLAN) (C3), Universal Mobile Telecommunication System (UMTS) (C3), Global System for Mobile communication (GSM) (C3,C4), General Packet Radio Service (GPRS) (C3), Wireless Fidelity (WiFi) (C3), Bluetooth (C3), Zigbee (C3), infra-red communications (C3), Industrial, Scientific and Medical radio band communications (ISM) (C3)
Data Storage	Cloud (C1,C2,C3,C4,C5)

1.1 Dependability of Time Critical Remote Monitoring Systems

In this section, a definition for dependability for TCRMSs is obtained in terms of reliability, security and privacy. Then, the existing failure conditions that degrade the dependability are discussed. Based on the potential failures, necessary reliability requirements are inferred.

1.1.1 Definitions

From [Avižienis et al. 2004], dependability is defined as the ability to deliver a service strictly within the specified requirements in terms of availability, reliability, safety, confidentiality, integrity and serviceability (maintainability). For a particular application, emphasis can be on different attributes based on the requirements. According to the International Organization for Standardization, the standard ISO 8402, reliability is defined as, *the ability of an item to perform a required function, under given environmental and operational conditions and for a stated period of time.* [ISO8402 1994]. The term *item* represents any component, subsystem or such entity. A required function may be a single function or a combination of different functions necessary to provide a specified service. A failure occurs when a system is not capable to perform a required function or a set of functions [Rausand and Høyland 2004]. The meaning of capability here can be identified based on the specific scenario or the application.

Availability denotes the ability of an entity (under combined aspects of its reliability, maintainability and maintenance support), to perform its required function at a stated instant of time or over a stated period of time (British Standard - BS4778) [Rausand and Høyland 2004]. According to the document published by National Institute of Standards [Kissel 2013], following definitions are obtained. Security is defined as, *"A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprises risk management approach."*. Confidentiality is defined as the ability to control the disclosure of data to a specific party and nobody else. It is such that even if an authorized party receives the data, it cannot be utilized in terms of its content. Privacy is defined as the non-disclosure of data beyond relevant or authorized parties. Authentication is defined as the verification of the identity of a user, process, or device, often as a prerequisite to allow access to resources in an information system. Authorization is defined as the process or the acts of granting access privileges to a user,

program, or process.

Reliability denotes the ability of an entity to continue to maintain its specifications over its operational life-time [Høyland and Rausand 2009]. Reliability is generally referred to as, failure free operation of an entity (a system, subsystem or a component). The reliability may be measured in different ways depending on the selected attributes, as listed under the definition of dependability. General measures include mean time to failure (MTTF), number of failures per time (unit failure rate), the probability that the item does not fail in a time interval (*0, t*] (survival probability), the probability that the entity is able to function at time *'t'* (availability at time *'t'*). However, for a TCRM application, the performance measures may vary depending on the specific communication and data access needs.

1.1.2 Current Issues in Time Critical Remote Monitoring Systems

According to [Rausand and Høyland 2004], for any system, it is necessary to identify the functions (or categories of functions/operations) to characterize its possible failures. For a TCRMS, there are several essential functions: *data generation, data transmission, data storage and data access* (Figure 1.1). Investigation of this thesis is limited to data access and transmission. In addition to the failures, a failure mode is defined as the scenarios in which it is not possible to fulfill a required function (or a set of functions) [Rausand and Høyland 2004]. In general, for any system, different types of failure modes may occur: failure during operation, failure to operate at a prescribed time, failure to cease operation at a prescribed time and spurious premature operations. In this section, the failure modes which cause delays in each of the essential functions of a TCRMS are described (Table 1.2). Since the existing TCRMSs use secure cloud storages, it is assumed that the operational failures during data access is solely accounted by the failures during the data access. Therefore, it is reasonable to assume that the cloud storages are highly reliable data hosts.

Data Generation - In the data generation stage, a sensor reads a physical parameter and converts it into a corresponding electrical signal. Once it is appropriately processed

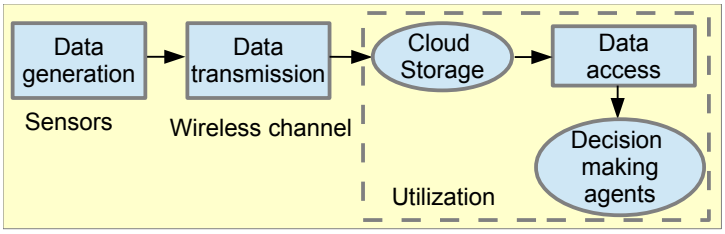


Figure 1.1: Three Essential Functions in a TCRMS.

it becomes the data output of the sensor. Examples for failures modes (or the scenarios) in data generation include, failure of the sensor, failure of the processing circuit or the firmware [Akyildiz et al. 2002][Ye et al. 2003]. In this thesis, it is assumed that the installed sensors complete the expected operational life-time such that the potential failures are at a minimum.

Data transmission - In the transmission stage, data is transmitted from the sensor to the secure cloud storage over wireless channels. This thesis will focus on unreliable band limited wireless channels. Functional requirements for data transmission in TCRMSs include,

1. gaining access to the channel
2. secure transmission of data and
3. minimum latency between the source and the secure cloud storage.

Examples of specific failure modes include channel failures due to fading, transmission circuitry failures, synchronization errors etc. Dependability of data transmission requirements in terms of reliability and security can be summarized as,

1. Reliability [Rausand and Høyland 2004]
    a) guaranteed reception of the data
    b) non-repudiation (inability to deny transmission or reception by either party)
2. Security [Stallings 2006]
    a) confidentiality

b) integrity

c) authenticity

Focus of this thesis shall be emphasized on the functional failure modes of data transmission in terms of reliability, security and latency [Agarwal 1991] [Angrisani et al. 2003]. The delay causing factors include, delays due to encryption, insufficient residual energy for transmission, framing, channel access, channel hand-off, transmission, propagation and queuing.

Data Storage - For brevity, it is assumed that there are sufficient cloud storage such that availability does not get hindered.

Data Access - Most significant functional requirement of secure data access minimizes latencies associated with authentication, authorization and context-aware access management. In this thesis, the context is described based on the point of access and the situation (e.g. during and emergency). The main failure modes includes inability to verify the authenticity of an intruder from a legitimate user during an impersonation (or mimicry), granting access to an unauthorized agent due to an incorrect decision [Yu et al. 2010] [Zissis and Lekkas 2012] [Sathiamoorthy et al. 2013]. An example would be the failure to verify sufficient attributes of an agent/user identity due to resource (computational and/or bandwidth) constraints [Jensen 2012] [Chadwick and Inman 2013] [Arias-Cabarcos et al. 2012a] [Thomas et al. 2008] which may cause repeated authentication attempts. Other undesirable outcomes resulting in accidental privileged access [Brucker and Petritsch 2009] [Ray and Ray 2014] [Bartsch 2010] can be exploited by an attacker mimicking the identity of a privileged user [Premaratne et al. 2010a] or due to mis-management of permission overrides.

The Table 1.2 shows a summary of the failures for each function and the corresponding failure modes. In summary, according to the British Standard 5760-5 cited in [Rausand and Høyland 2004], the failure modes for each of the two essential functions (i.e. data transmission and access) of TCRMSs correspond to the type of *failures during operation*. Based on the above definitions, it is possible to describe dependability as the ability of a TCRMS to operate (or function) as expected in a reliable and secure manner during

Table 1.2: Summary of failure modes in TCRMSs for the three essential functions: Data generation, data transmission and data access.

Sub-system	Functional Failure During Operation
Data Generation	- Loss of device (sensor) availability - hardware failure, software failure, external hazards - Loss of security due to data not being encrypted.
Data Transmission	- Channel failures - Transmission device failure - Latency
Data Access	- Inability to validate identities. - Authorization violations - Access control latency

data transmission and access. As evidenced by the potential failures in TCRMSs, the failure minimizations during transmission over insecure (or vulnerable), unreliable wireless channels and data access over unreliable distributed systems are necessary to be declared as a reliable TCRMS.

1.2 Limitations of the Existing Solutions

In this section, the limitations of existing solutions that can be used to minimize the failure conditions in Section 1.1.2 are discussed.

Cognitive radio networks are effective solutions to utilize sporadically available radio spectrum, however, the channel availability is uncertain. A feasible solution would be to increase the accuracy is spectrum sensing [Pham et al. 2009] [Cheng et al. 2012] [Deng et al. 2012] [Akyildiz et al. 2011]. Depending on the application and the choice of network architecture, applicable spectrum sensing techniques vary. In overlay network architectures, cooperative spectrum sensing techniques offer greater accuracy to detect vacant and occupied channels [Akyildiz et al. 2011] [Yücek and Arslan 2009]. Among cooperative spectrum sensing techniques, the accuracy of decision of the selected users determine the accuracy of the final decision on channel availability [Selén et al. 2008] [Malady and da Silva 2008] [Wang et al. 2014a]. Another significant problem within the scope of cooperative spectrum sensing is the possibility of falsifying the spectrum availability data by a malicious agent [Duan et al. 2012] [Hyder et al. 2012]. Therefore, it is

necessary to formulate strategies which can reliably select the set of users to cooperate on spectrum sensing. In addition, when there are interruptions due to the licensed user arrivals, efficient hand-off techniques [Wang et al. 2010][Song and Xie 2012][Wang et al. 2012][Sheikholeslami et al. 2015] are proposed. However, development of delay sensitive mechanisms to manage the spectrum hand-off is still an open research problem.

For secure data transmission from sensors, physically unclonable function (PUF) based robust encryption solutions have been proposed [Selimis et al. 2011] [Guajardo et al. 2008]. The level of security is determined by the complexity of the encryption key which in turn depends on the number of bits [Meguerdichian and Potkonjak 2011a]. In a sensor with a limited energy reserve, computationally intensive encryption may results in rapid energy drain and ultimate failure of the transmission device [Meguerdichian and Potkonjak 2011a] [Wang and Tehranipoor 2010]. Managing the trade-off between encryption and energy usage is a challenging task. Energy efficient route selection is desirable when it is necessary to aggregate certain remote monitoring data in a distributed TCRMS. Although there are various energy efficient routing metrics [Chang and Tassiulas 2004][Ok et al. 2009][Liu et al. 2012] , the investigations on the impact of the encryption key size and the residual energy of the sensors is an open research topic.

Reliability of user authentication for data access in cloud computing infrastructure is hindered due to poor digital identity management [Gopalakrishnan 2009] [Cox 2012]. Cloud based federated identity management is more suitable to provide efficient access for distributed users [Zwattendorfer et al. 2013] [Birrell and Schneider 2013] [Dreo et al. 2013]. Unreliability of identity management depends on the delayed response of the digital identity providers and the limitations of the expressiveness of identity disclosure policies [Yan et al. 2009] [Arias-Cabarcos et al. 2012a] [Ghazizadeh et al. 2012]. The development of effective strategies to minimize the communication delays of the identity providers and at the same time to enhance the expressiveness of the disclosure policies is an open research problem [Squicciarini et al. 2008].

Under unreliable conditions, the authentication of a user itself cannot sustain effective authorization enforcements due to context dependencies [Almutairi et al. 2012] [Zissis and Lekkas 2012] [Fernandes et al. 2014], shared use of computing devices as well as emerging

practices such as bring-your-own-device [Wang et al. 2014b] [Miller et al. 2012] [Scarfo 2012]. Sole use of location dependent authentications, and device specific authentications fail in the above scenarios [Sampangi and Hawkey 2016] [Margaria et al. 2014]. Due to such inherent unreliable conditions, it is necessary to incorporate additional measures to perform authorizations that account for context dependent access requests. The challenge is to develop innovative solutions to help the authorizations to be fail-safe provided that there are verifiable security metrics to associate with a specific application dependent context [Jonsson and Olovsson 1997] [Pamula et al. 2006] [McQueen et al. 2006] [Tupper and Zincir-Heywood 2008] [Premaratne et al. 2008] [Premaratne et al. 2010b].

1.3 Thesis Research Questions

The main research objective of this thesis is to propose effective novel solutions for secure and reliable data transmission and access for TCRMSs. The research questions are formulated based on the reliability aspects stated in Section 1.1.2 and to address the limitations discussed in Section 1.2. In the first research problem the reliable time-critical data transmission over opportunistic cognitive radio networks is addressed. In the second research problem, energy efficient secure data transmission using low power sensors is addressed. The third and fourth research questions address the requirements of reliable identity management for efficient user authentications and context-dependent authorization enforcements in cloud computing infrastructure respectively.

1.4 Contribution

The contribution of this thesis can be summarized as:

- The development of a novel multi-attribute trust based cooperative spectrum sensing mechanism for reliable channel detection in cognitive radio sensor networks. The proposed solution detailed in Chapter 3 is more reliable compared to randomly selected coalition based cooperative spectrum sensing techniques in the presence of malicious secondary users (SUs). The reliability is enhanced primarily by designing a

mechanism to reliably select the most trustworthy set of secondary users to perform the cooperative spectrum sensing. New evidence based trust metrics are defined and used to identify three types of spectrum sensing data falsification attackers based on their attack profiles in order to distinguish the genuine secondary users. *Content published in Adhoc Networks [Premarathne et al. 2016]..*

- The development of an innovative delay bounded re-entrant spectrum access model based on renewable counting process. The proposed solution detailed in Chapter 4 is more reliable compared to existing hand-off mechanisms where transmission delay constraints on the number of possible hand-offs are not considered. *Content is under review - Adhc Networks, Elsevier.*

- The development of a novel energy efficient physically unclonable functions (PUF) based secure data transmissions over the sensed spectrum channels. The proposed solution described in Chapter 5 is more reliable due to energy aware PUF key size determination, which minimizes the probability of partial re-identification of the key. This solution is more appropriate to provide minimum security guarantees to support selective data encryption for secure transmissions over the sensed wireless channels. *Content published in Pervasive and Mobile Computing [Premarathne et al. 2015c].*

- The development of novel reliable trust metrics to identify the most trustworthy identity providers to participate in the trust negotiations with federated identity management in cloud platforms. The proposed solution detailed in Chapter 6 enhances the reliability by selecting the most trustworthy identity providers based on the novel metrics. These novel trust metrics are sufficiently descriptive in terms of the secure availability and to reveal the extent of agreement of the credential disclosure policies. Furthermore, the proposed solution has been mapped to an existing quality assurance model for trust based authentications in cloud computing infrastructure. *Content published in IEEE Transactions in Cloud Computing [Premarathne et al. 2015a].*

- The development of a situation-specific authorization enforcement mechanism for TCRMSs using a novel context-aware disclosure risk metric. To control the disclosure risks under unreliable conditions, a novel location dependent disclosure risk metric based context-aware authorization enforcement mechanism is described in Chapter 7. The use of this metric to enforce situation specific authorizations based on Rumpole [Marinovic et al. 2014], a Belnap logic based framework, is described and compared with the existing logic frameworks. In comparison, the proposed solution offers more flexibility to enforce situation-specific break-the-glass rules for more robust access control. *Content published in Computer Networks [Premarathne et al. 2015b].*

Overall, this thesis resulted in the following publications.

1. U. S. Premarathne, I. Khalil, and M. Atiquzzaman. Secure and reliable surveillance over cognitive radio sensor networks in smart grid. *Pervasive and Mobile Computing*, 22, 3-15, 2015. Special Issue on Recent Developments in Cognitive Radio Sensor Networks.

2. U. S. Premarathne, I. Khalil, and M. Atiquzzaman. Trust based reliable transmission strategies for smart home energy management in cognitive radio based smart grid. *AdHoc Networks*, 41, 15-29, 2016. Special Issue on Cognitive Radio Based Smart Grid The Future of the Traditional Electrical Grid.

3. U. Premarathne, I. Khalil, Z. Tari, and A. Zomaya. Cloud-based utility service framework for trust negotiations using federated identity management. *IEEE Transactions on Cloud Computing*, 5:2, 290-302, 2015.

4. U. S. Premarathne, I. Khalil, and M. Atiquzzaman. Location dependent disclosure risk based decision support framework for persistent authentication in pervasive computing applications. *Computer Networks*, 88, 161-177, 2015.

1.5 Thesis Organization

The remaining chapters in this thesis are organized as follows. In Chapter 2, the existing literature on failure preventive techniques for TCRM data transmission and data access are surveyed. This is followed by Chapter 3, which describes a trust based user selection method for reliable cooperative spectrum sensing in cognitive radio networks. In Chapter 4, a delay analysis of the interruptions on reliable opportunistic data transmissions is described. Then, in Chapter 5, a novel energy efficient PUF based secure TCRM data transmission mechanism is described. In Chapter 6, an effective trust based identity provider selection mechanism for reliable user authentications in cloud platforms is described. In Chapter 7, an innovative context-aware authorization enforcement model to handle the situation-specific TCRM data access requests is described. Finally, Chapter 8 concludes the thesis.

CHAPTER 2

Related Work

This chapter describes the related background information to understand the contributions of this thesis. This includes the preliminaries of cognitive radio networks (CRNs), wireless sensor networks (WSNs), cloud computing, pervasive computing aspects.

2.1 Background

Most TCRMSs are pervasive computing applications with distributed sensor networks which transmit the sensed data over wireless channels. The remote monitoring data are stored and accessed over distributed cloud platforms to facilitate reliable time-critical decision making processes.

2.1.1 Wireless Sensor Networks

Wireless sensor networks contain nodes (or individual embedded systems) that are capable of (1) interacting with the environment, (2) processing information locally (e.g. encryption, data aggregation), and (3) communicating this information over wireless channels [Akyildiz and Vuran 2010]. Each node has a sensing mechanism (or a sensor), a microprocessor, and a transceiver. The sensor captures data from a physical phenomenon. The on-board microprocessors can be programmed to perform complex tasks including data encryption and transmission. The transceiver provides wireless connectivity to communicate the observed phenomena and to transmit the sensed data on the dedicated wireless

channels. The sensor nodes are generally stationary and are powered by limited capacity batteries. As a proactive measure to prolong the lifetime, the sensor nodes may switch-off the transceivers and essentially become disconnected from the network. Although it minimizes the energy consumption, it is a major challenge to provide connectivity of the network in TCRM applications. When the sensor node is damaged or has very little residual energy, depending on the TCRM application, it may be cost-prohibitive to replace each exhausted battery or even impossible to install new sensors with minimum latency (e.g. hostile environments, large coverage distances or areas) [Min et al. 2014][Bruyneel and Ninane 2014]. Therefore, when designing for a specific application, it is important to address the core requirements which needs to be satisfied to ensure a failure-free operation in a wireless sensor network [Karlof and Wagner 2003] in terms of energy efficiency, availability and data integrity.

2.1.2 Cognitive Radio Networks

According to Federal Communications Commission [Tadaion 2004], a CRN is defined as, a radio or a system that can sense its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify the system operation, such as to maximize throughput, mitigate interference, facilitate interoperability, etc. In a CRN there are two types of users: primary users (PUs) and secondary users (SUs) [Akyildiz et al. 2006] [Akyildiz et al. 2011]. A PU has the higher priority or legacy rights to access a certain part of the spectrum. A SU has a lower priority than the PU but the SU can exploit the opportunity to use that part of the spectrum when the PU does not transmit.

In a CRN, at a particular time-slot, if the channels are not occupied by the PUs, these are available for the SUs to transmit [Akyildiz et al. 2008] [Akan et al. 2012]. For this spectrum reuse functionality, the SUs have to sense the radio channels [Li et al. 2012b]. Spectrum sensing is the task of obtaining awareness about the spectrum usage and existence of PUs in a geographical area. If it is observed that the PU is active, the SU will have to vacate the channel immediately or within a certain amount of time. Failure to

accurately detect the presence of a PU and a vacant channel, decreases the reliability of SU transmissions. Therefore, spectrum sensing has significant importance in CRNs to make reliable decisions for accessing the vacant channels. In CRNs, when an interruption on the current channel is detected, the transceivers adapt to continue the active communications over the newly detected vacant channels. This operation is known as spectrum hand-off [Wang et al. 2010] [Song and Xie 2012].

Cognitive radio capabilities may also be exploited by wireless sensor networks (WSNs), which otherwise employ fixed spectrum allocations. Due to the congestion in dedicated spectrum, cognitive radio based wireless sensor networks are useful for various delay-sensitive remote monitoring applications. In general, a cognitive radio sensor network (CRSN) [Akan et al. 2009] can be defined as a distributed network of wireless cognitive radio sensor nodes, which sense signals and collaboratively communicate their readings dynamically over available spectrum bands in a multihop manner to ultimately satisfy the application-specific requirements [Khan et al. 2016][Tragos et al. 2013][Akyildiz et al. 2008]. Informative discussions on cognitive radio based wireless sensor networks are provided in [Khan et al. 2016] and [Tragos et al. 2013].

2.1.3 Pervasive Computing

Pervasive computing (also called ubiquitous computing) is the interaction of everyday objects to communicate information by being constantly connected and available [Henricksen et al. 2002] [Satyanarayanan 2001]. This interaction is provided based on the data generated by the sensors attached or embedded in these objects. Data communication is facilitated through the wireless networks. Pervasive computing applications are more environment-centric compared to web-based or mobile computing. Therefore, pervasive computing applications which require remote monitoring data collection and analyses can be conveniently characterized as a TCRMS. Examples include, pervasive health monitoring systems [Abawajy and Hassan 2017], scalable cloud based data and service management [Maler and Reed 2008][Xia et al. 2016].

2.1.4 Cloud Computing

Cloud computing is established as a successful utility computing paradigm [Dastjerdi and Buyya 2014][Buyya et al. 2010][Moreno et al. 2014]. Utility based cloud computing provides packaged computing resources (e.g. storage, software development platforms) as a metered service (e.g. subscriptions, utility based pricing) [Dastjerdi and Buyya 2014][Buyya et al. 2010]. With the advent of pervasive computing concepts such as the Internet-of-Things (IoT) [Atzori et al. 2010][Gubbi et al. 2013][Botta et al. 2016][Palattella et al. 2016], essential features of utility based cloud computing services include offloading, delegating and outsourcing certain tasks on to the cloud platform. For TCRMSs, cloud platforms provides an excellent choice as secure data storage hosts [Cummins 2017][Netbiter 2017]. Capacity to hold huge volumes of data and the ability to facilitate distributed access further strengthens this choice.

2.2 Limitations of Existing Solutions on Reliable Data Transmissions

As mentioned before, delays associated with the remote monitoring data transmission and access are among the main hindrances for dependability of accurate time-critical decision making in the TCRMSs. Primarily, the data transmission delays are caused due to channel unavailability and the interruptions. Delays associated with the distributed data access is caused due to the latencies during the distributed user authentications using the digital identities as well as during authorization decision making. In this section various existing solutions to minimize the above mentioned delays are discussed.

Most of the existing wireless networks use a fixed spectrum assignment policy [Akyildiz et al. 2006]. Main disadvantages of such assignments include a large portion of the assigned spectrum being sparsely utilized. According to Federal Communications Commission [FCC 2003], this variation in spectrum utilization ranges from 15% to as high as 85%. Existing issues and concerns related to the limited available spectrum and the inefficiency in the spectrum usage demands new communication solutions to exploit the

existing wireless spectrum opportunistically [Akhtar et al. 2016] [Kwon et al. 2017]. This requirement has resulted in NeXt Generation (xG) Networks, Dynamic Spectrum Access (DSA) and cognitive radio networks [Akyildiz et al. 2006][Akyildiz et al. 2011][Mitola and Maguire 1999].

2.2.1 Spectrum Availability Detection

Spectrum sensing is the task of detecting vacant channels for the SUs to transmit. Alternatively, in a CRN, failure-free channel access depends on the accurate detection of the vacant spectrum in which there are no active PUs. In [Akyildiz et al. 2011][Axell et al. 2012][Reyes et al. 2016][So and Sung 2016][Li et al. 2017] detailed discussions are provided on various spectrum sensing techniques. Generally, in primary transmitter detection based spectrum sensing, a weak signal is detected through local observations. Three schemes that are commonly used for transmitter detection include matched filter detection, energy detection, and feature detection [Akyildiz et al. 2011][Axell et al. 2012]. Due to the lack of interactions between primary users and secondary users and interferences such as the hidden terminal problem, the primary transmitter detection techniques alone may not be sufficient to achieve accurate spectrum sensing [Akyildiz et al. 2006][Akyildiz et al. 2008][Yücek and Arslan 2009][Akyildiz et al. 2011][Cheng et al. 2012]. Delays associated with spectrum sensing result in latencies for channel access for the sensors to transmit the sensed data. To overcome the above said limitations and to increase the detection accuracy, cooperative spectrum sensing techniques have been developed [Akyildiz et al. 2011][Axell et al. 2012][Reyes et al. 2016][So and Sung 2016].

In cooperative spectrum sensing, a group of SUs participate to sense the spectrum. Based on these local decisions, an aggregated decision is computed by using pre-defined rules (e.g. AND rule, OR-rule, Majority rule) [Akyildiz et al. 2011]. When the OR rule is used, if there is atleast one user to indicate the channel is vacant, the decision fusion center declares the spectrum available. The majority rule requires at least a half of the cooperative users to report the channel as being vacant. For the AND rule, all the cooperating users have to indicate the channel as being vacant. Due to decision fusion, the accu-

racy of the aggregated decision is more accurate than the individual spectrum availability decisions. However, cooperative spectrum sensing may provide less accurate results on spectrum availability detection due to spectrum sensing data falsification (SSDF) attacks [Duan et al. 2012]. In these SSDF attacks, the local spectrum sensing data are maliciously altered to generate erroneous results which results in false detection or miss detection. A false detection occurs when it is declared that the channel is occupied when it is in fact not being used by the PUs. A miss detection occurs when the SUs are not being able to detect the vacant channels when the PUs are in fact not transmitting (or PUs are inactive). Erroneous spectrum availability decisions contribute to the overall delays in the data transmission.

To reduce the impact of spectrum sensing data falsification attacks, trustworthiness of the participating SUs is a significant concern for reliable cooperative spectrum availability detection [Selén et al. 2008]. Existing user selection methods consider the location and fading characteristics of the participating secondary users and provide less focus on computing the trustworthiness of SUs [Peh and Liang 2007][Malady and da Silva 2008]. Literature review on the specific cooperative user selection criteria will be discussed in Chapter 03.

2.2.2 Spectrum Hand-off Management

Spectrum hand-off is necessary to sustain the data transmission of a SU when it is interrupted due to the arrival of a PU [Wang et al. 2012]. For an interrupted SU, the spectrum hand-off mechanisms allow access to a suitable channel which is available with minimum waiting time. When the waiting time is longer, the transmission delays become much larger. These subsequent spectrum allocations can be done based on: reactive, proactive and hybrid spectrum hand-off management strategies [Wang et al. 2012]. In reactive spectrum hand-off management, the SU is allowed to access the spectrum on the next available channel in an on-demand manner. In proactive spectrum hand-off management, the SU is allowed to access a predetermined channel by estimating the probability for it to be vacant. These two approaches have been quantitatively compared in [Wang et al. 2011].

However, it is more reliable to establish the connection in proactive hand-off management as the availability can be pre-determined before the connection is established. In hybrid spectrum hand-off schemes, the reactive and proactive schemes are combined by using the proactive spectrum sensing and reactive hand-off action.

Existing proactive spectrum hand-off management solutions [Song and Xie 2012] [Song and Xie 2010] offer more reliable probability estimations based on previous channel utilization statistics. On the other hand, existing reactive spectrum hand-off management schemes the reliability of finding a vacant channel completely depend on the spectrum sensing accuracy. In [Nguyen et al. 2013], the authors propose a proactive spectrum hand-off method to reduce the number of hand-offs with minimum switching time between the channels for a SU. To perform the dynamic hand-off process, a channel sequence is pre-defined. In addition, to initiate a spectrum hand-off, following conditions should be satisfied (i) PU is non co-existent and (ii) the common control channel strength is higher than a pre-defined threshold. However, in [Nguyen et al. 2013], the feasibility of a hand-off also depends on a maximum tolerable delay bound. In Chapter 04, specific spectrum hand-off management techniques related to multiple interruptions in cognitive radio networks are discussed.

2.2.3 Residual Energy-Aware Sensor Data Transmission

In wireless sensor networks, energy consumption of the sensors in relation to secure data transmission is discussed focusing on secure routing mechanisms to avoid attacks such as crippling attacks, sink holes, hello floods [Karlof and Wagner 2003][Kuthadi et al. 2016]. To sustain the operational life-time of a sensor, energy harvesting mechanisms have been proposed to replenish atleast some of the depleting energy [Alippi et al. 2009][Zhang et al. 2013b][Wu et al. 2015]. In addition, radio optimization mechanisms including transmission power control, modulation optimization, cooperative communications, energy efficient cognitive radios are proposed [Feng et al. 2013][Rault et al. 2014]. In a TCRM application, apart from enhancing the operational life-time of the sensors, the ability to perform secure data transmissions over an expected period of time is vital. Existing work on energy

management in cognitive radio sensor networks include, (i) sleep/awake scheduling for cooperative spectrum sensing [Deng et al. 2012][Cheng et al. 2012][Xu and Liu 2008][Pham et al. 2009], (ii) scheduling to access available spectrum [Bayhan and Alagoz 2013], (iii) adaptive cluster based operations [Deng et al. 2012], (iv) energy harvesting mechanisms [Park et al. 2012][Wang et al. 2015] and combinations of above mentioned strategies [Hoang et al. 2014]. For a CRSN with cooperative spectrum sensing energy efficiency is a significant operational aspect. In [Pham et al. 2009], optimal number of cognitive sensors participating in the cooperative spectrum sensing is computed while minimizing the total energy consumption of the cooperative sensing. In [Bayhan and Alagoz 2013], the authors propose an energy efficient heuristic scheduler to manage spectrum access to ensure prolonged network life-time but the associated energy depletion due to secure data transmission using a suitable encryption mechanism is not considered.

However, in cognitive radio sensor networks, energy-efficient secure data transmissions should consider the energy expenditure in a sensor to perform the required sensory and data encrypting operations. In Chapter 05, energy efficient route selection methods and the significance of residual energy for CR sensors are discussed further.

2.2.4 Secure Data Transmission in Sensors

Secure data transmission over unreliable wireless channels is vital for TCRMSs. Inaccurate data reception causes delays due to repeated data transmissions and even corruption or loss of accurate sensed data. These lapses cause to degrade the dependability of the TCRMS [Gungor et al. 2013][Ma et al. 2013]. Since the sensors have limited computational power lightweight encryption techniques with sufficiently strong security is necessary.

Recently, secret key pre-distribution techniques have been proposed for secure data transmissions in wireless sensor networks [Henry and Stinson 2011][Knox and Kunz 2012]. Main limitation of this approach is when new sensor nodes are added on to the network, keys have to be updated. Also, when existing nodes are removed from the network, the keys have to be revoked. Thus, increase the complexity of managing a large sensor network with key pre-distributions. Random key pre-distribution schemes assume that

a sensor node is able to accurately verify the identity of a sender, which makes it a rather weak security enforcement. For example, radio frequency fingerprint [Henry and Stinson 2011] [Bonne Rasmussen and Capkun 2007][Knox and Kunz 2012] can be used to identify a sensor based on the physical characteristics of the wireless signals. However, it is not unique for every sensor and the identification accuracy depends on the classification technique employed [Knox and Kunz 2012].

Recent work on secure sensor data transmissions propose PUF based secure key generation and deployment schemes [Selimis et al. 2011][Guajardo et al. 2008]. PUF based keys are highly secure as these cannot be forged since the responses are generated with hardware inherent noise characteristics which are unclonable [Rührmair et al. 2010]. However, the PUF-based key should be sufficiently large enough to sustain a reasonable operational life-time of a sensor. In [Wei and Potkonjak 2012], authors describe minimizing energy leakages in order to reduce the vulnerabilities based on hardware Trojan attacks. This work considers the energy efficiency aspect but it has little relevance to facilitate key size selection based on th residual energy content. In [Meguerdichian and Potkonjak 2011b], energy efficiency of PUF based key generation in sensors is studied using existing models on delay and aging of hardware. However, this work does not indicate how the adjustments are made to reduce the energy losses due to data transmission over unreliable wireless channels. PUF based cryptographic device identification applications have been proposed for wireless sensor networks [Guajardo et al. 2008], RFID systems [Bolotnyy and Robins 2007][Guajardo et al. 2009], secure storage applications [Kursawe et al. 2009]. However, PUF based authentications with energy expenditure awareness have not been explored in CRSN based time-critical applications. In Chapter 05, specific secure sensor data transmission mechanisms using physical unclonable functions are discussed.

2.2.5 Sensors using PUF for Remote Monitoring Applications

In wireless sensor networks, PUF based node authentication is desired compared to standard sensor node authentication schemes, such as the Security Protocol for Sensor Networks (SNEP), due to the wireless channel unreliability [Yang et al. 2011]. In [Yang

et al. 2011], PUF based mutual node authentication scheme is proposed for delay tolerant wireless sensor networks. In [Mahapatra et al. 2015], optical PUF based secure data transmission in wireless body sensor networks are described. The dark current variation of photodiodes is used to generate the PUF key for encryption. In other applications such as in body sensor network [Lee et al. 2013], PUF generated challenge-response values are used for mutual authentications among the nodes. In addition, each node needs to complete the hashed and MAC operations in the verification process. Authors in [Meguerdichian and Potkonjak 2011b], matched PPUF (public key PUF) proposes a low power single clock cycle energy consumption scheme for mutual authentication of sensors (or low energy devices). During the authentication, to match two mPPUF keys, it is expected that both the parties use the same aging and disabling procedures in order to match the corresponding gate delays. The proposed scheme complements this work by considering the transmission and encryption functions and the residual energy constraints in determining the PUF key size. In [Wei and Potkonjak 2012], hardware Trojan attack detection scheme based on, power profiling, time, location and PUF is proposed for wireless sensor networks. PUF is used to authenticate a particular sensor as a trust measure to verify the validity of the power profile of the sensor at a particular location. In [Delvaux and Verbauwhede 2014], sensors are useful for remote monitoring applications when the helper data are protected such that the pattern reproducibility is minimized. The attack scenarios described in [Delvaux and Verbauwhede 2014] reveal that it is vital to consider the pattern reproducibility issue when the secure data transmissions rely on PUF based keys.

In addition to node authentication PUF is integrated with the sensor to sense the ambient environmental variations to guarantee the veracity of the sensed value [Gao et al. 2017]. The authors assume that, (i) the sensor with PUF is located in a hostile environment, (ii) the wireless communication channel is insecure, and (iii) no complex crypto module relying on stored secret keys is involved. In [Gao et al. 2017], it is shown that response bits reproduced consistently for a given environmental condition can track the changes in environmental parameters in a repeatable manner. PUF based sensor nodes are also used as trusted anchors for secure data transmissions. In [Haider et al. 2016], PUF based trusted sensor is an anchor to ensure integrity, authenticity and non-repudiation

guarantees on the sensed data when mobile devices are used in participatory sensing for IoT applications. The trusted PUF sensor serves as secure key storage for the digital signatures and secure boot processes.

Based on the above discussion, it is evident that although the PUF based solutions are proposed for wireless sensor based remote monitoring applications, energy efficient key size selection problem so as to minimize the probability of reproducibility (e.g. to guess a few or all of the consecutive bits in a key) has received very little attention.

2.3 Limitations of Existing Solutions on Reliable Data Access

2.3.1 Cloud based Identity Management Models

Authentication and authorizations for data access in TCRM applications can be efficiently managed over distributed cloud platforms. A summary of different cloud identity management (IDM) models is given in Table 2.1.

According to Birrel et al [Birrell and Schneider 2013], existing identity management systems can be categorized based on their functionality as i) single-sign-on, ii) federated identity and iii) anonymous credentials. In a federated system, multiple distinct identities are used to authenticate a single user to a service provider. In cloud, the user identities may be residing in multiple IDPs. These IDPs may reside i) within or ii) outside the domain of cloud service provider [Almutairi et al. 2012]. In [Arias-Cabarcos et al. 2012b], a taxonomy is proposed to classify the risks involved in facilitating collaborations over federated identity management. The main objective of this risk computation framework is to enhance the ability to provision various cloud services.

Cloud based identity management is essentially controlled by a set of administrative and provisioning policies [Gopalakrishnan 2009]. These policies may vary across different cloud domains and based on the way they collaborate [Almutairi et al. 2012]. Therefore, identity management in cloud is challenging due to the i) heterogeneity of the visibility and scope of attributes, ii) multiple user accounts with different application and service

Table 2.1: Summary of Classifications of Cloud Identity Models

Reference	Model	Description
Gopalakrishnan [Gopalakrishnan 2009]	Trusted IDM pattern	ID system runs on a trusted cloud based domains (e.g. private cloud).
	External IDM Pattern	Public clouds. ID system is external to the cloud service providers' domain.
	Interoperable IDM Pattern	Can use different authentication technologies for multiple service providers.
Cox [Cox 2012]	First Model	Cloud service provider generates and manages identities.
	Second Model	Different systems synchronize to manage identities and the cloud services.
	Third Model	Cloud service provider use the federated identities of the organizations.
Cloud Service Alliance	Hub-and-spoke model	Identities are managed centrally by a broker or a proxy.
	Free-form model	Cloud service provider manages identities generated by several identity providers.
	Hybrid model	Combination of the advantages of the above two models.
Zwattendorfer [Zwattendorfer et al. 2013]	Identity in the Cloud Model	Cloud service provider generates, authenticates and manages identities.
	Identity to the cloud	ID system is external to the cloud service providers' domain.
	Identity from the cloud	Identity provider entirely within the domain of the cloud service provider. Similar to the Identity-as-a-Service model [Emig et al. 2007]

providers, iii) inter-operation of different types of identity attributes, iv) service launch and termination conditions and v) notifications and updates of active and inactive vs trustful and untrusted entities at the network level.

Recently, authors in [Adams et al. 2011] have proposed a receipt mode trust negotiation protocol with load balancing and encrypted proxy certificates for secure and trustworthy communications. There are other computing offloading techniques based on cost graphs, pointer analysis techniques, partitioning techniques based on efficiency, environmental changes, application specific requirements [Deng et al. 2015]. However, these techniques are performance oriented with little consideration on the reliability requirements. Since the digital user identities are highly privacy sensitive data, trust between

the identity provider and the cloud utility service provider is vital. Moreover, when trust negotiations are offered as a utility based service, the reliability of the negotiations has to be maximized while the failure rate, due to interruptions should be minimized. Therefore, the cooperativeness of the identity providers in disclosing the credentials is vital. Based on the above discussion, in facilitating IDM as a cloud utility service, the above mentioned challenges should be accounted strategically in order to ensure reliable trust negotiations based authentication services in TCRM applications. In Chapter 06, federated identity management models, the related risk assessment frameworks and the trust evaluation methods are discussed.

2.3.2 Disclosure Control of Data

In TCRMSs, disclosure of sensitive information can occur in two ways: identity disclosure of the users and attribute disclosure of the stored data (e.g. health data of patients, critical measurements of electrical generation units in smart grids, smart meter data etc) [Hundepool et al. 2012]. Existing disclosure risk measures offer to preserve privacy depending on the collective disclosure of certain attributes. The disclosure risks are computed using statistical properties of data (e.g. frequency of occurrence, mean, mode, variance, Hamming distance between the data points in spatial representations). Time-critical remote monitoring applications may require situation aware data utilization demands such as access from different locations and pervasive computing devices. Such situation dependent data access requirements in TCRMSs may result in unintended disclosure of sensitive data [Shilton 2009][Kotz 2011][Chakraborty et al. 2012].

Statistical disclosure control aim to protect by controlling the release of data to prevent link between different attributes of sensitive data [Hundepool et al. 2012][Willenborg and De Waal 2012]. Assessing the disclosure risks and implementing disclosure controls are equally important [Domingo-Ferrer and Mateo-Sanz 2002]. Existing disclosure risks include k-anonymity [Truta and Vinay 2006], t-closeness [Li et al. 2007], l-diversity [Machanavajjhala et al. 2007], distance based record linkage measures [Torra et al. 2006][Shlomo 2014] consider the content but does not use the contextual information

(e.g. time, location) or the situation specific information. An effective disclosure control method would be to restrict the authorizations to access the sensitive data [Hundepool et al. 2012] based on the contextual or situation specific requirements. This approach is apt for a TCRMS since the situation-specific data access requirements demand more flexible yet robust access control.

2.3.3 Disclosure Risk Measures

In Table 2.2 categorization of different types of disclosure risk metrics is shown.

Table 2.2: Disclosure Risk Measures

Feature	Metrics	Purpose
Record linkage	Distance based metrics (Euclidean distance, Mahalanobis distance Manhattan distance [Torra et al. 2006], [Torra 2000], Kernel distance, Choquet integral based distance [Abril et al. 2012b]), Probabilistic record linkage metrics [Shlomo 2014]	To identify the link between data.
Similarity based membership	k-anonymity [Samarati 2001], l-diversity [Machanavajjhala et al. 2007] and t-closeness [Li et al. 2007]	To reveal the existence of sensitive attributes
Entropy	Entropy based metrics [Willenborg and De Waal 2012][Bezzi 2007][Domingo-Ferrer et al. 2001][Antal et al. 2014][Airoldi et al. 2011]	To quantify the extent of information loss
Statistical disclosure control	aggregation [Kokolakis and Nanopoulos 2001], rounding [Domingo-Feffer et al. 2002], swapping [Dandekar et al. 2002], adding random noise to data	To reduce disclosures based on statistical measures of the data

Main drawback of these disclosure risk measures is that the extent of revealing sensitive information is solely dependent on the content of the data. It is not possible to incorporate the context of the data utilization to provide a more holistic measure on the disclosure risk. In identity disclosure risks are associated with records and files. Risk measures assess the extent for an intruder can match the identities directly or indirectly. File level risks measure the average risk across the entire file based on population uniqueness [Duncan et al. 2011]. Population uniqueness is defined as the proportion of individual data that has unique values on a set of variables. Conventional use of perturbed protection

methods (e.g. statistical disclosure control protection methods [Nin et al. 2010]) apply only to the non-confidential attributes leaving the confidential attributes. Attributes based disclosure risk estimations attempts to find the extent of risk for an intruder to identify an individual by using identifiers or a combination of quasi-identifiers. Attributes based disclosure risk is measured using (i) distance based or (ii) probabilistic record linkage techniques. However, these techniques do not consider the contextual dependencies for risk estimation [Abril et al. 2012a].

2.3.4 Risk based Authorization Models

In TCRMSs, depending on the situation, permissions on data access may have to be changed. Stating separate rules for each type of emergency (or critical) situations would complicate the authorization policies. Therefore, permission over-rides are employed to effectively manage necessary exemptions to facilitate situation specific data access needs.

The recently published risk aware authorization model in [Gasparini 2013] proposes an obligatory model to be accountable for access permits. However, there is no guarantee to ensure the user obligations. Recently, a dynamic sensitivity based access control model was proposed by [Harel et al. 2010]. The authors in [Harel et al. 2010] use a metric called the M-score to estimate the potential risk of mis-usability of a data item by incorporating the quality of information, quantity of information exposed and the amount of effort to identify data. M-score can be used for tabular data. Also, the authors in [Harel et al. 2010] do not consider the location or such contextual dependency in estimating the disclosure risk of data.

In [Cheng et al. 2007], fuzzy multi-level security model is used to make the authorization decisions. The authors propose an economic perspective in solving the access control problem by quantifying risk as a mode of currency that is expendable. They optimize the legitimate access control decisions based on risk by using an equivalent fuzzy controller. However, they do not consider the contextual dependencies in evaluating the risk.

In [Dimmock et al. 2004], trust and risk based role based access control model is presented. They measure trust for a specific principal to perform a particular action.

Cost-benefit analysis is performed to evaluate the amount of trust that is necessary to offset the risk associated with the intended actions to be performed in the initial user request. Then, this trust measure is compared with a cost and generates a predicate. The predicate is used with role based access control in open systems to produce the authorization decisions.

Recently, a similar cost based risk evaluation is proposed by extending the widely accepted role based access control [Chen and Crampton 2012]. In [Molloy et al. 2009], risk is treated as a finite resource which can be quantified as a liability for performing an action. For a particular access request, the risk is calculated based on the known information, such as the previous access history logs. Each request will bare a price which is quantified based on risk units. So for a denial access request the price will be infinite. Since the user is unable to pay-off the risk, the request is denied. However, in this model the authors do not have explicit consideration on the context dependencies associated with each access request.

On the other hand context dependent access control models [Zhang and Parashar 2004] [Kulkarni and Tripathi 2008] [Wang et al. 2009] have been proposed to account for smart environments to ensure accurate authorizations. Location changes are also considered as a contextual change that characterize the dynamic user behaviors. However, the risk of an authorization and a permission override (e.g. break-the-glass rules or permission overrides) to access shared data resources and risk variability due to change of context (e.g. location, time and situation) has not been explored in existing models. In Chapter 07, the logic frameworks to specify the break-the-glass authorizations and the associated metrics for computing the context-related risks are discussed.

CHAPTER 3

Multi-Attribute Trust based Reliable Transmission Over CRSN

3.1 Outline of the Chapter

This chapter describes a reliable user selection method for cooperative spectrum sensing as a reliable strategy to access the vacant channels in a CRN. For TCRMSs, channel accesses with minimum delays are vital to ensure reliable data transmissions. Compared to other existing techniques, cooperative spectrum sensing offers greater accuracy to detect vacant channels by aggregating the local decisions of the cooperative secondary users. However, the accuracy of detecting the vacant channels is reduced due to the presence of false local sensing data injected by malicious spectrum sensing data falsification (SSDF) attackers.

Main contribution of this chapter is a novel multi-attribute trust metric which is capable of (i) selecting the most trustworthy cooperative users and for (ii) identifying the non-malicious users in the presence of three types of spectrum sensing data falsification attackers. Part of the content of this chapter is published in [Premarathne et al. 2016].

This chapter is organized as follows. In Section 3.2 limitations of the existing solutions and the research problem are described. In Section 3.3, the notations used in this chapter are summarized. Next, in Section 3.4 the multi-attribute trust metric, its functional form and the reliability analysis are described. In Section 3.5 multi-attribute trust based user selection for cooperative spectrum sensing is described. Reliability of the trusted user

selection is further analysed in Section 3.5.2 and Section 3.6 where the non-malicious user are identified in the presence of both cooperative users and the potential spectrum sensing data falsification attackers. Finally, this chapter concludes with Section 3.7.

3.2 Introduction

In cognitive radio networks, for a secondary user (SU), spectrum sensing is vital to detect if a channel is vacant to begin data transmission. When the primary user (PU) is not transmitting on a channel, it is considered as a vacant channel. Inaccurate spectrum sensing, when the PU is transmitting, causes interferences to the PU resulting in transmission failure. On the other hand, inaccurate spectrum sensing when the PU is not active, prevents the SU from transmitting resulting in reduction of the spectrum utilization. Thus, accurate spectrum availability decision making with true spectrum sensing data is vital prevent transmission failures to both PUs and SUs. For TCRMSs, accurate spectrum sensing is crucial to reduce delay sensitive data transmission failures due to channel unavailability [Akan et al. 2012][Shah et al. 2013][Malady and da Silva 2008][Suryadevara et al. 2015].

Among different spectrum sensing techniques [Akyildiz et al. 2011], cooperative spectrum sensing provides far more accurate results due to the aggregation of local decisions on spectrum sensing [Zhang et al. 2009] [Akyildiz et al. 2011][Yu et al. 2012][Lee 2015]. In Chapter 02, Sections 2.1.2, 2.2.1 and 2.2.2 describe the significance of spectrum sensing, the cooperative spectrum sensing technique and how the decision fusion using pre-defined rules, can improve the accuracy of the spectrum availability decisions. Moreover, cooperative spectrum sensing is advantageous compared to other spectrum sensing techniques when the cognitive radios experience independent fading or shadowing [Akyildiz et al. 2011]. Also, with cooperative sensing, it is possible to overcome the hidden primary user problem with fusion of local decisions to reduce the collisions which in turn decreases the spectrum utility [Akyildiz et al. 2011]. To make the final spectrum availability decision, the fusion center (FC) collects the individual sensing information from the users, identifies the spectrum holes and broadcasts this information over a control channel to the other

SUs.

3.2.1 Cooperative Sensing Strategies

In this section, different types of cooperative spectrum sensing strategies [Zhang et al. 2009][Akyildiz et al. 2011] [Yu et al. 2012] are discussed.

- Sequential cooperative sensing - Users sequentially sense each channel one after another. This approach increases the detection accuracy and more suitable when there are unpredictable channel conditions. However, it takes a long time to complete the sequential spectrum sensing.

- Parallel cooperative sensing - As opposed to sensing all the channels, each user senses different channels in one sensing period. This strategy aims to improve the channel sensing efficiency rather than the detection accuracy. Channel states can be sensed in a much shorter time compared to the sequential strategy.

- Semi-parallel cooperative sensing - FC uses a beacon signal to communicate with the cooperating SUs. All the cooperative SUs sense the channels synchronously over the sensing time. Once a channel is detected to be free, FC signals to cease further spectrum sensing. A selected source SU informs the FC with the index of the available channel.

- Non-consensus based cooperative spectrum sensing - The fusion center only considers the spectrum sensing reports from one-hop neighbors but not from the entire network.

- Consensus based cooperative spectrum sensing - The fusion center consider the spectrum sensing reports from all users or the entire network. Takes a longer time to compute the final decision compared to the non-consensus based fusion scheme.

Sequential, parallel and consensus based cooperative spectrum sensing techniques are not reliable as these may fail completely due to one or more inaccurate spectrum sensing decisions. Such failure is more pronounced when there are malicious spectrum sensing

data falsification (SSDF) attackers [Hyder et al. 2014] [Hyder et al. 2012] [Duan et al. 2012]. Semi-parallel cooperative sensing method with non-consensus decision making is more suitable for spectrum sensing in TCRMSs as it offers greater control to select a set of cooperative users based on a pre-defined selection criterion. Using consensus based schemes, the delays associated to make the final decision at the FC becomes larger as the spectrum sensing local decisions for the entire network is required.

Accuracy of cooperative spectrum sensing depends on the aggregated decision result for detecting the presence of a PU in a channel (Q_d) and the aggregated decision result for falsely declaring the presence of PU in a channel (Q_f). The two measures Q_d and Q_f depend on the local decisions, $P_{d,j}$ and $P_{f,j}$ respectively [Akyildiz et al. 2008] [Akyildiz et al. 2006]. For the j^{th} SU, $P_{d,j}$ is the probability of detection of the presence of a PU when actually transmitting. $P_{f,j}$ is the probability of falsely declaring the presence of a PU when the channel is vacant. The probability of misdetection for the j^{th} SU is defined as $P_{m,j} = 1 - P_{d,j}$. In addition, it is also important to consider the rules on how the aggregated sensing results are used to formulate the final decision. The decisions of each cooperative user is combined using well known majority rules (i.e. logical AND or OR rules) [Akyildiz et al. 2011] to make the final decision on channel availability. In addition to these rules, a trust based fusion scheme has been proposed in [Wang et al. 2016a]. In this scheme, the trustworthy users are identified based on the overall trust value computed using the trust gain (or loss) when true (or false) spectrum sensing data are reported. Based on the above discussion, it is evident that the accuracy of the cooperative spectrum sensing largely depends on the credibility or trustworthiness of the cooperative users to provide true spectrum sensing data.

3.2.2 Reliability of Cooperative Spectrum Sensing

In TCRMSs, reliability of channel access for delay sensitive data transmissions is measured in terms of the accuracy of spectrum sensing. For example, in smart grid remote monitoring systems, the delays in accessing the wireless channels cause a significant impediment to transmit the delay sensitive data [Bicen et al. 2012b][Ma et al. 2013]. High accu-

racy of spectrum sensing is vital to reduce the channel access delays in order to support delay-sensitive data transmissions [Li et al. 2012a]. The accuracy of cooperative spectrum sensing depends on the trustworthiness of the cooperating SUs as to provide true data [Duan et al. 2012]. In addition, the accuracy of spectrum detection can be hindered due to the inefficiency of spectrum detection technique [Akyildiz et al. 2006][Akyildiz et al. 2008], poor signal conditions (e.g. due to fading, shadowing) or malicious interruptions, such as SSDF attacks [Hyder et al. 2014] [Hyder et al. 2012] [Duan et al. 2012]. If it is assumed that the channel conditions do not vary drastically, false spectrum sensing data contributes largely to inaccurately detect the available channels.

As mentioned in Chapter 2 Section 2.2.1, malicious SSDF attacks cause a grave threat to hinder the accuracy of spectrum sensing. The impact of SSDF attacks contributes to two failure scenarios. The first issue is the inability to use available spectrum due to false declaration of the PU activity when in fact the PU is not transmitting any data. The second issue is the occurrence of collisions when allowing the SU to transmit when in fact the PU is transmitting data. Any of these failures cause delays to access the vacant channels for data transmissions in TCRMSs. Significance of the SSDF attacks increase the total transmission delay as the opportunities in subsequent time slots are missed due to the inaccurate spectrum availability decisions. Among the possible solutions to prevent such failures include the selection of genuine users to participate in cooperative spectrum sensing. Trust measures are stated as a justifiable measure for SSDF attack resilience [Duan et al. 2012]. In order to distinguish between the genuine and the malicious users, appropriate trust measurements (or metrics) are necessary. Based on the selected measurements, the genuine SUs can be distinctly identified among potential SSDF attackers. Trust computation is generally used to evaluate the reliability of an entity [Duan et al. 2012][Qin et al. 2009] [Chatterjee and Chatterjee 2015]. The trustworthiness of cooperative users is a critical factor which significantly contributes to the accuracy of the local spectrum sensing decisions as well as how these are combined [Duan et al. 2012].

3.2.3 Limitations of Existing Cooperative User Selection Methods

Existing solutions which helps to distinguish the genuine (or non-malicious users) from the SSDF attackers (or the malicious users) mainly focus on user selection methods. Different types of user selection methods include trust and reputation based clustering [Hyder et al. 2014], penalty based cooperation strategies [Duan et al. 2012] [Chatterjee and Chatterjee 2015] as well as optimal decision fusion strategies [Cai et al. 2014]. Most of the optimal decision fusion strategies use additional information such as distance, channel conditions etc. Summary of the existing user selection methods for cooperative sensing are compared in Table 3.1.

Most of the user selection criteria (see Table 3.1) are capable of reducing the negative impacts on channel conditions, such as correlated shadowing and fading, to improve the accuracy of spectrum sensing. However, the trustworthiness of the SUs has not been quantitatively estimated as a potential measurement to select genuine users for cooperative spectrum sensing. The contributions described in this chapter bridge this research gap by proposing a novel multiple-attribute based trust metric for reliable user selection for cooperative spectrum sensing.

In the three trust based schemes [Vosoughi et al. 2014], [Guo et al. 2015] and [Wang et al. 2016a] proposed for selecting the honest users among the SSDF attackers, the trust is computed based on the previous spectrum sensing results (or the interaction history). All three schemes distinguish the malicious and non-malicious users based on the trust values marked using a pre-defined threshold value. Trust based weighted sensing results aggregation presented in [Qin et al. 2009] is the most closely comparable with the proposed solution. The authors propose a trust based framework for cooperative spectrum sensing. Trust computation for each SU is based on a Beta distribution using two behavioural rating attributes. Malicious and non-malicious users get different reputation values based on the previous behaviour ratings. The positive rating characterizes honest behaviour while negative rating characterizes the dishonest behaviour. Unlike the proposed multi-attribute trust metric ($MATM$), to compute the reputation in [Qin et al. 2009], these two types of behaviours have to be explicitly stated in terms of positive and negative ratings.

Table 3.1: Existing User Selection for Cooperative Spectrum Sensing.

Selection Feature	No. of Attributes	Ability to Characterize SSDF Attacks
shadow correlation, location[Selén et al. 2008]	2	Depends on the channel state characteristics.
location [Malady and da Silva 2008]	1	-
distance between the FC and the SU [Najimi et al. 2013]	1	-
distance between the PU and SU [Han et al. 2010]	1	-
channel gain under Rayleigh fading [Sun et al. 2007]	1	-
location, received PU power [Guo et al. 2009]	2	Limited ability depends on the available PU characteristics.
largest channel gain [Wei and Zhang 2010]	1	-
cooperation footprint based on spatial diversity [Mishra et al. 2006]	1	-
Cost function based on transmission energy, sensing energy and detection probability [Najimi et al. 2013]	3	-
Reputation based cluster selection: sensing history, initial reputation, votes between clusters based on channel status and the distance between the node and the median of the cluster [Hyder et al. 2014]	3	Limited to individual and collaborative SSDF attacks. Specific attack behaviors are not characterized using the reputation metric.
Trust based on past behaviour as positive rating, negative rating [Qin et al. 2009]	2	Use Beta distribution for de-centralized reputation computation.
Trust-aware gossip-based scheme [Vosoughi et al. 2014]	1	Useful for consensus based spectrum sensing with push-sum gossip protocol to eliminate the involvement of SSDF attackers.
Trusted social behaviour inspired clustering scheme [Guo et al. 2015]	1	Identify the honest users based on the inter-cluster and intra-cluster friendship values.
Trust scheme based on D-S evidence theory [Feng et al. 2015]	1	Reliability function to compute the trust and to identify the trustworthy users based on the previous spectrum sensing results.

The novel multi-attribute trust metric described in this chapter complements that of [Qin et al. 2009] based on (i) the evidence based trust computation using three attributes and (ii) the ability to distinctly characterize three SSDF attack types rather than just consider as a dishonest behaviour in general.

3.2.4 Contributions

The main contributions of this chapter are described as follows.

- *Novel multi-attribute trust metric ($MATM$) for user selection for cooperative sensing* - A novel multi-attribute trust metric using three trust attributes is proposed. The three trust attributes are computed based on the history of incorrect spectrum sensing data instances, responses received by the FC and the number of attempts for channel access. This contribution differs significantly from the existing user selection strategies as three distinct evidence based trust attributes are selected to compute the trustworthiness of a SU instead of using only the previous spectrum sensing results.

- *SSDF attack behaviour characterization using the expressiveness of the three attributes of $MATM$.* It is demonstrated that $MATM$ is sufficiently expressive to describe the three SSDF attack behaviours distinctly. Reliable identification of malicious users and non-malicious users are demonstrated. This contribution significantly differs from existing solutions as the three evidence based attributes characterize the SSDF behaviors based on the value of $MATM$ and probabilistic local spectrum sensing decision accuracy measures (i.e. $P_{f,j}$ and $P_{d,j}$).

  Based on the simulation experiments, $MATM$ provides an accuracy upto 100% to distinctly identify the non-malicious users in the presence of SSDF attackers. Thus, provides a promising metric to distinctly identify trustworthy users in the presence of SSDF attackers and to enhance the reliability of cooperative spectrum sensing decision making.

3.3 Notations

Notation	Description
τ	duration of the sensing time
λ	the threshold of the decision statistic (either Q_f or Q_d) below which the hypotheses are invalid
t_r	local sensing result reporting time
T	frame duration
$p(h0)$	prior probability of the absence of a PU
$p(h1)$	prior probability of the presence of a PU
$G_Q()$	Gaussian Q-function
var	variance of a Gaussian variable
γ	signal-to-noise ratio
f_s	channel frequency
NR	total number of local spectrum sensing decisions
ch	channel
$H0$	decision hypothesis for the presence of a PU in ch
$H1$	decision hypothesis for the absence of a PU in ch
$P_{d,j}$	probability of detection of the j^{th} SU
$P_{m,j}$	probability of misdetection of the j^{th} SU
$P_{f,j}$	probability of false alarm of the j^{th} SU
$P_{d,j}(\lambda, \tau)$	probability of detection of the j^{th} SU for a given τ and λ
$P_{f,j}(\lambda, \tau)$	probability of false alarm of the j^{th} SU for a given τ and λ
Q_d	aggregated decision result for detecting the presence of a PU in ch
Q_f	aggregated decision result for falsely declaring the presence of PU in ch
$\bar{Q_d}$	aggregated decision result for detecting the presence of a PU in ch for a given τ

$\bar{Q_f}$	aggregated decision result for falsely declaring the presence of PU in ch for a given τ
A_1, A_2, A_3	trust attributes where A_i where $i = 1, 2, 3$ at t
A_1^*, A_2^*, A_3^*	trust attributes where A_i where $i = 1, 2, 3$ at $(t - \tau)$
$t, t1, t2$	time, two time instances where $t1 < t2$
X_j	number of false spectrum sensing data samples from the j^{th} SU
$X_{total,j}$	total number of spectrum sensing data samples received at FC from the j^{th} SU
$D_{rsp,j}$	number of responses received from the j^{th} SU
$Resp_j$	total number of requests sent from FC to the j^{th} SU
$I_j(ref)$	degree of greediness of the j^{th} SU
$I_j(mean)$	average greediness
a_j	number of channel allocations for the j^{th} SU
r_j	number of channel access requests from the j^{th} SU
FGF	forgetful factor
$u(MATM)_j$	utility of $MATM$ of the j^{th} SU.
$u(A_i)$	utility of each trust attribute A_i
$k_{scale,i}$	scaling constant where $0 < k_{scale,i} < 1$ and $\sum_i k_{scale,i} = 1$ for the i^{th} attribute.
TC	trusted coalition
T_{thr}	threshold of $u(MATM)$ for TC selection
$\binom{NR}{l}$	l number of local spectrum sensing decisions out of NR (where $\frac{NR}{2} < l < NR$)
$E_{residual,j}$	residual energy of the j^{th} SU
E_{th}	the limiting amount of residual energy required for secure transmission
ED	energy detection threshold
Beta (a_1,b_1)	Beta distribution with parameters a_1 ad b_1

Gamma (a_2,b_2)	Gamma distribution with parameters a_2 and b_2
Weibull (a_3,b_3)	Weibull distribution with parameters a_3 and b_3
Lognormal (a_4,b_4)	Lognormal distribution with parameters a_4 and b_4
KLD	Kullback-Leibler divergence

3.4 Multi-Attribute Trust Metric

In this section, the proposed multi-attribute trust metric is derived and the reliability of the metric is analyzed. It is assumed that a centralized spectrum availability decisions are made at a fusion center (FC) by combining the local decisions of the trusted cooperative users according sets of pre-defined rules [Akyildiz et al. 2002][Akyildiz et al. 2006][Akyildiz et al. 2008][Akyildiz et al. 2011].

3.4.1 Overview of Trust Metrics

Trust may be termed as direct trust or indirect trust depending on the application scenario and the observations [Bertino et al. 2010][Thirunarayan et al. 2014][Zhao and Li 2013][Bhalaji and Selvaraj 2017]. Direct trust specifies the direct observations. Direct observations are also known as first hand information. An example would be the interactions between two entities in a network. Some of the interactions may be successful while some may be unsuccessful. Indirect trust specifies the indirect observation which are also referred to as second hand information. For example, the reputation scores given to entities in a network are useful measures of indirect trust. For the direct trust computations [Marsh 1994], the history of sensing decisions are used to compute the trustworthiness as the ratio between the correct sensing decisions and the total sensing decisions over a

period of time. Direct trust computations usually make use of historical data of previous interactions between two entities over a period of time.

A trust metric provides means to evaluate the subjective assessment among two entities to perform a particular action. Trust metrics can also be considered as functions which compute the trust values using quantitative or qualitative measures [Mahoney et al. 2005] [Marsh 1994]. For example, in wireless networks the trust can be measured based on the data packets forwarded, control packets forwarded, availability based on beacon messages, battery life-time, consistency of reported values, reputation responses etc [Movahedi et al. 2016] [Mali and Misra 2016] [Kerrache et al. 2016]. In cloud computing, certificate or tickets based trust mechanisms are used to establish the trust among the service providers and the authenticated users while the graph theoretic models and data ownership based information are used for the trust computation [Premarathne 2017][Werner et al. 2017] [Cusack and Ghazizadeh 2016]. Different types of trust metrics use numerous computational techniques. Arithmetic type trust metrics use simple mathematical operations to compute the trust values. Another example is the chain of proof type metrics, which perform validations as a chain of evidences. Each validated link (i.e. between a pair of users) contributes to the validation of the entire chain. In probabilistic type of measures, the trust is computed using probabilities by preserving the total probability principle.

3.4.2 Trust Attributes

Trust is essentially a multi-dimensional feature which can be described by a set of attributes corresponding to each of the selected dimensions. To compute multi-dimensional trust, multiple attributes are necessary [Das and Islam 2012][Luo et al. 2010][Li et al. 2010][Li and Du 2013]. Once the multiple attributes are identified, the functional form of the combination of these attributes need to be computed. In [Keeney 1974], an attribute is defined as a dimensional space. An attribute can take values in this dimensional space. Using the multi-attribute utility theory [Keeney 1974][Keeney 1972], based on the dependencies between these attributes, a suitable functional form is derived.

The proposed multi-attribute trust metric is composed of three attributes A_1, A_2, A_3

corresponding to three dimensions. These three dimensions characterize the trustworthiness of a SU are as follows:

- SU provides accurate sensing decisions to the FC upon request
- SU responds with the local sensing decisions and
- SU genuinely request to access the spectrum for data transmission.

To determine the direct trust of a cooperative SU, the first trust attribute (A_1) is computed based on the probability of falsifying the spectrum sensing data during time "t", by using previously detected such incorrect data over a fixed time window.

$$A_1 = \frac{X_j}{X_{total,j}} \tag{3.1}$$

where X_j denotes the number of instances where the spectrum sensing data were false and $X_{total,j}$ represents the total number of correct spectrum sensing data sent by the j^{th} SU during a a fixed time duration. Larger the value of A_1 reflects more trustworthiness. Possible values of A_1 include a maximum of 1 and a minimum of 0. It is assumed that a cooperative SU using the energy detection technique for PU detection [Akyildiz et al. 2011]. The values of X_j and $X_{total,j}$ can be computed using the interaction history data stored at the FC. The spectrum availability decision is stated based on a pre-defined threshold for energy detection method [Akyildiz et al. 2011]. At the FC, it is also assumed that based on the overall decision, each individual local spectrum sensing data is classified as a correct or false sensing data.

Next, the second attribute A_2 is selected to characterizes the responsiveness of a SU. It is assumed that when the FC request for local sensing data, a responsive SU will send the spectrum sensing result. It is assumed that the SU has a good reception of the control channel to receive the request from the FC. Failure to respond is considered as an indication of an untrustworthy user.

$$A_2 = \frac{D_{rsp,j}}{Resp_j} \tag{3.2}$$

where $D_{rsp,j}$ and $Resp_j$ denote the number of responses received from the j^{th} SU and the total number of spectrum sensing requests received by the j^{th} SU respectively. Larger the value of $A2$, the trustworthiness is high. Possible values of A_2 includes a maximum of 1 and a minimum of 0. It is assumed that the communications in terms of responses and requests are recorded in the form of a response record matrix at FC. Rows and columns of the matrix corresponds to responses and requests.

Next, the third trust attribute (A_3) is computed based on the history of channel access requests. When a SU indicates the requirement to transmit the data, a channel is allocated for a SU if it is vacant at time t. The term *relative greediness* is used to characterize an SU to harness more spectrum resources for transmission based on the spectrum allocation success rate. It is assumed that when some SUs do not get a chance to transmit in a particular time slot, they have greater demand to transmit in the next time slot. Such persistent behaviour for accessing a channel is characterized as greed.

$$A_3 = \frac{I_j}{I_{mean}} \tag{3.3}$$

I_j represent the degree of greediness and I_{mean} represent the mean degree of greediness over a fixed time period. To compute the value of I_j, the average signal strength over that fixed time period T and the failure rate of channel allocation is taken into account. This is equivalent to the computation of current trust using a forgetful factor (FGF) [Das and Islam 2012]. The forgetful factor is included to express the relative staleness of the ratio of average signal strength during the fixed time period. In [Das and Islam 2012], it is generally assumed to be $FGF = 0.9$ which indicates that the ratio does not vary drastically.

$$\begin{aligned} I_j &= FGF \times (\frac{a_j}{r_j}) \\ I_{mean} &= \frac{\sum_{j=1}^{K} I_j}{K} \end{aligned} \tag{3.4}$$

where a_j and r_j represents the number of times in which channels were allocated and data transmitted by the j^{th} SU and total number of requests made by that SU to access a channel respectively. The ratio between a_j and r_j represents the indirect trust [Marsh

1994] based on the channel allocation history. The values of a_j and r_j are computed based on the channel allocation history data at FC for the j^{th} SU over the time period T. The value of I_{mean} is computed as the average of I_j for $j = \{1, 2, \cdots, K\}$ over T. Larger the value of $A3$, the user is more reliable. Possible values of A_3, is a maximum of 1 and a minimum of 0.

In addition to the above trust attributes, a direct trust measure based on the residual energy of each SU is also considered. For a SU, if the residual energy content is greater than a pre-defined threshold, the SU is considered to be trustworthy in terms being operational without failure. When selecting the trusted set f SUs, this direct trust is also considered (see Section 3.5).

3.4.3 Functional Form of Multi-Attribute Trust

A utility function quantifies the preference by assigning a numerical value to indicate the satisfaction of a particular criterion [San Cristóbal 2012]. According to [Akyildiz et al. 2011], when the cooperative users are selected using different strategies, the utilities of the selections vary. Also, the impact of preferences (i.e. $k_{scale,i}$ in Equation 3.6) among the trust attributes vary. Next, the utility of $MATM$ is computed using the multi-attribute utility theory [Keeney 1972]. The three main steps [San Cristóbal 2012] to compute the utility value of $MATM$ are, (i) to determine the utility functions for each attribute A_1, A_2 and A_3, (ii) verification of utility independence conditions, and (iii) identification of the functional form of the multi-attribute utility function for $MATM$.

To compute the functional form of $MATM$, multi-attribute utility theory is used [Keeney 1974]. According to [Keeney 1974], multiple dimensions of a metric is described using the corresponding attributes multiplicatively. Values taken by each attribute reflect the overall trust for an agent. In Equation 3.5, the three trust attributes A_1, A_2, and A_3 are used to express the multiple dimensions of the overall trust measure $MATM$.

$$MATM = A_1 \times A_2 \times A_3 \tag{3.5}$$

In order to compute a utility functional form for $MATM$, it is necessary to fulfill the

conditions stated in [Keeney 1974].

- Minimum number of attributes required to define the concept of *preferential independance* - According to [Keeney 1974], for preferential independence to be validated, atleast *three (03)* are required. Hence, the selection of A_1, A_2, A_3 would suffice.

- Utility independence of A_1, A_2, A_3 for all possible scenarios - There are two main scenarios that arise are, (i) when there is sufficient signal strength or (ii) when there is insufficient signal strength to receive a request to cooperate with spectrum sensing local decision. In (i), A_1, A_2, A_3 are utility independent. These utilities only depend on the time (e.g. at what time the SU receives, responds and when the response is received.). In (ii), utility of A_2 and A_3 are not independent of each other since the responsiveness depends on the reception of the request. On the other hand, A_1 is utility independent of A_2 and A_3. Therefore, it can be concluded that utility independence among the three attributes are not preserved in all scenarios.

- Preferential independence of A_1, A_2, A_3 for all possible scenarios. Either scenario (i) or (ii) exists at a particular time. For the same scenarios (i) and (ii) described above, the preference for each attribute is independent as there is no existence of a conditional preference relation between the attributes on their individual computations respectively (see Equations 3.1, 3.2, and 3.3).

According to the conditions satisfied above, Theorem1 proved in [Keeney 1974] is satisfied to confirm the utility of $MATM$ of the j^{th} SU (or $u(MATM)_j$) takes an additive functional form stated as follows (Equation 3.6).

$$u(MATM)_j = \sum_{i=1}^{3} k_{scale,i} u(A_i) \tag{3.6}$$

For each utility function $u(A_i)$, a scaling constant $k_{scale,i}$ is defined as $0 < k_{scale,i} < 1$ such that $\sum_i k_{scale,i} = 1$ [Keeney 1974]. The value of $k_{scale,i}$ is subjective as it depends on the particular scenario. It is selected as a qualitative value which represents the most and least desirable attributes for that particular scenario. Then, the utility functions $u(A_i)$ for A_1, A_2, A_3 are described.

- For A_1, the variation of the utility is considered to linearly degrade (from 1 to 0) as the ratio $\frac{X_j}{X_{total,j}}$ (in Equation 3.1) varies from 0 to 1. Utility is a maximum when there data is not found to be false atleast once. Since A_1 is a direct trust computation based on past behaviour of truthfulness of the responses, $A_1 = 0.5$ is considered as the point where $u(A_1)$ is 50% [Das and Islam 2012].

- For $A2$, the variation of the utility is considered to linearly increase (from 0 to 1) as the ratio $\frac{D_{rsp,j}}{Resp_j}$ (in Equation 3.2) varies from 0 to1. Utility is a maximum when the SU responds to all the requests received from the FC. Since $A2$ is a direct trust computation based on the past behaviour of responsiveness, $A2 = 0.5$ is considered as the point where $u(A2)$is 50% [Das and Islam 2012].

- For $A3$, the variation of the utility is considered to be a sigmoid function which has the highest utility when the channel conditions are equally good or better at the j^{th} SU (when compared to FC). It is assumed that FC have good signal conditions for sensing channel ch, therefore, the ratio given in Equation 3.3 has a maximum of 1 and a minimum of 0. For simplicity it is considered that the utility linearly varies from 0 to 1 when the ratio (A_3) varies from 0.5 to 1 respectively. It is also assumes that utility will be 50% when $A_3 = 0.75$ [Das and Islam 2012].

3.5 Trusted User Set for Cooperative Sensing

In this section, the reliability of selecting a trusted set of users based on the $u(MATM)$ is described. A *trusted coalition (TC)* (Equation 3.7) is defined as the set of SUs participating in cooperative spectrum sensing.

$$TC = select(([u(MATM)_j], NR, T_{thr})\text{and}(E_{residual,j} \geq E_{th})) \tag{3.7}$$

where $j = 1, 2, \cdots, NR$ is the number of SUs. The function *select* is the decision making function. This function assigns the j^{th} SU as a member of TC if the utility value is greater than T_{thr}, which is a pre-defined threshold value ($T_{thr} \in [0, 1]$), and if that SU has sufficient energy reserves. $E_{residual,j}$ is the amount of residual energy of the j^{th} SU and it should be greater than the minimum required (E_{th}) for a secure transmission.

3.5.1 Impact of TC Selection on Cooperative Spectrum Sensing Decision Formation

When the binary local decisions (or sensing data) are reported to the FC, fusion rules are applied to obtain the cooperative decision [Akyildiz et al. 2011]. The fusion rules combine the local decisions (or sensing data) to make the cooperative decision at the FC. For a given $P_{d,j}$ and $P_{f,j}$ the generalized fusion rules (see Equations 3.8) states that correct primary user detection is declared if the decision statistic is greater than a threshold λ. Majority AND rule is selected since it is assumed that atleast some of the users of the TC have detected the signal (or sensed the channel). Therefore, it is important to note that $\frac{NR}{2} < l < NR$ local decisions are used in the fusion rules.

$$P\{decision = H1|H1\} = P\{Q_d > \lambda|H1\}$$
$$P\{decision = H1|H0\} = P\{Q_f > \lambda|H0\}$$

where,

$$Q_f = \sum_{l=k,j}^{NR} \binom{NR}{l} P_{f,j}^{l}(1 - P_{f,j}^{NR-l})$$
$$Q_d = \sum_{l=k,j}^{NR} \binom{NR}{l} P_{d,j}^{l}(1 - P_{d,j}^{NR-l})$$

where Q_f and Q_d are the aggregated sensing decision results for the false declaration of the presence and the actual presence of a PU in the channel ch at the FC. λ is the threshold of the decision statistic (either Q_f or Q_d) below which the hypotheses are invalid. For example, in [Qin et al. 2009], the threshold for $\lambda > 0.65$ is considered. $H1$ and $H0$ denote the hypotheses of absence or presence of primary user in a particular frequency band and $P_{f,j}$ and $P_{d,j}$ are the individual decision associated accuracy measures for the j^{th} SU. In this chapter, it is assumed that energy detection is used to detect the presence of a PU [Feng et al. 2015]. In energy detection, if the energy of the detected signal is above a threshold, then it is declared that the PU is present. The accuracy of the decisions for $H1$ and $H0$ is determined by $P_{d,j}$ and $P_{f,j}$ respectively. The FC declares the spectrum

available if all the cooperative users decisions indicate as available. When the OR rule is used, if there is atleast one user who indicates the channel as being vacant, the FC declares it as available. The majority rule requires at least a half of the cooperative users to report the channel as being vacant. These simple fusion rules can be generalized to the l out of the NR rule (see Equations for Q_f and Q_d in 3.8). When l is taken as 1 and NR, the l out of NR rule becomes the OR and AND rule respectively. The majority rule can be obtained from the l out of NR rule under the condition when $l \geq \frac{NR}{2}$.

3.5.2 Characterization and Identification of Spectrum Sensing Data Falsification (SSDF) Attack Behavior using MATM

In this section, the $MATM$ is used to characterize the spectrum sensing data falsification attack behaviors. The three types of SSDF attack behaviors [Cai et al. 2014] that are used for the analysis are described below.

- *Always-on attack* where the malicious user always sends "1" to indicate that the channel is occupied by the PU. A selfish user can benefit from this and wastes the spectrum resource.

  It is assumed that the channel sensing period may be varied. Therefore, the responsiveness of a cooperative user depends on the varied sensing period. An *Always-on* attacker, is excessively greedy in terms of gaining channel accessibility. Since the response is always a 1, maximum value of A_3 is 1. This attacker does not fail to respond, the value of A_2 can also take a maximum of 1. The attacker always report that the PU is in operation, the value of A_1 during a sensing period will be equivalent to $P_{f,i}$. Therefore, knowing the possible values of A_1^*, A_2^*, A_3^*, the expected values of these attributes (i.e. A_1, A_2, A_3) are computed as shown in the Table 3.3.

- *Always-off attack* where the malicious user always sends "0" to indicate that the channel is vacant when in fact it is occupied by the PU.

  The attacker responds during each spectrum sensing, the value of A_2 will remain as 1. The attacker aims to disrupt the utility of the spectrum resource by falsely

Table 3.3: $MATM$ Attributes based SSDF Attack Behaviour Representation. Updated Attributes at times $t, (t-\tau)$ are denoted as A_i and A_i^* respectively.

Behaviour	Updated Attributes		
	A_1	A_2	A_3
Always-on	$\frac{A_1^*+P_{f,i}}{2}$	$\frac{A_2^*+1}{2}$	$\frac{A_3^*+1}{2}$
Always-off	$\frac{A_1^*+(1-P_{f,i})}{2}$	$\frac{A_2^*+1}{2}$	A_3^*
Always-false	$\frac{A_1^*+(P_{f,i}+P_{m,i})}{2}$	$\frac{A_2^*+1}{2}$	$\frac{A_3^*+0.5}{2}$
Trusted SU	$\frac{A_1^*-P_{d,i}}{2}$	$\frac{A_2^*+1}{2}$	$\frac{A_3^*-P_{a,i}}{2}$

indicating the channel to be available. Therefore, A_3 takes a minimum of 0. Since this attacker always indicate that the spectrum is vacant A_1 is equivalent to $(1-P_{f,i})$.

- *Always-false attack* always send opposite sensing results which causes both spectrum wastage and interferences for transmission.

  Since the attacker responds during each spectrum sensing, the value of A_2 will remain as 1. Since the attacker indicates the opposites of channel status (i.e. occupancy and the availability) the available channel gets misdetected and the occupied channel is falsely declared to be available. Therefore, A_1 takes the value of $(P_{f,i}+P_{m,i})$. Since the utility gain have equal probability to be used or not to be used, A_3 takes the value of 0.5.

- For a trusted SU, the expected behavior in terms of A_1, A_2 and A_3 can be described as follows. For A_1, the trusted SU is less likely to provide false spectrum sensing data. For A_2, responsiveness of a SU remains is at a maximum. For A_3, the greediness will increase as the SU gets access to available spectrum with a probability of access $P_{d,i}$.

Based on the above discussion, the three attack behaviors and the expected trusted user behavior characterized using $MATM$ is summarized in Table 3.3. Each behaviour is represented by the attributes A_1, A_2, A_3 at time t. Then, after a sensing time of τ, the updated attributes are represented as A_1^*, A_2^*, A_3^* (at time $(t-\tau)$). It is assumed that each SSDF attack behaviour is progressively computed using the three attributes of $MATM$.

3.6 Experimental Results and Discussion

In this section the suitability of the proposed metric for SSDF attacker identification and trusted cooperative user selection is analyzed. In addition, a delay analysis is described to demonstrate the variation of the accuracy of cooperative spectrum sensing decision with the sense time.

In the first experiment the usefulness of $MATM$ and the context-dependent trust metric proposed in [Qin et al. 2009] to holistically describe the three types of SSDF behaviors is compared. Next, the performance of Beta distribution based attack behaviour simulation using the behaviour characterization described in [Qin et al. 2009] and the three attribute of $MATM$ is compared.

3.6.1 Effectiveness of Characterizing SSDF Attack Behaviours to Identify the Malicious Users

The proposed $MATM$ is compared with the trust computation proposed in [Qin et al. 2009]. In order to do the comparison, the trust metric proposed in [Qin et al. 2009] is interpreted as follows.

The three SSDF attack behaviours and the trusted SU behavior corresponds to four different contexts which can be characterized by different positive and negative behavior scores [Qin et al. 2009]. $P_{f,j}$ is equivalent to $E1$ in [Qin et al. 2009] and $P_{m,j}$ (or $(1-P_{d,j})$ is equivalent to $E2$ in [Qin et al. 2009]. The authors state two context-dependent forget factors corresponding to Always-on and Always-off attack behaviours. Since the authors in [Qin et al. 2009] does not state the preferences of the context-dependent forget factors, it is assumed that an attacker will not change its behaviour between different types of attack behaviour. Also, it is assumed that an attacker does not exhibit more than one attack behaviour at the same time.

The attack behaviours were simulated by varying the attribute values as described in Table 3.3 to satisfy the malicious behaviours described in Section 3.5.2. The three attack behaviours are comparatively analyzed by fitting statistical distributions (Table 3.4) and

Table 3.4: Characterizing SSDF Attack Behaviour using $MATM$ - Compared the approximated distributions using Standard Error (SE) corresponding to the parameters of the specific distribution (where a_i and b_i (where $i = 1, 2, 3, 4$) are the parameters of the corresponding distributions).

Behaviour	SE of Approximated Distributions			
	Beta (a_1,b_1)	Gamma (a_2,b_2)	Weibull (a_3,b_3)	Lognormal (a_4,b_4)
Always-on	(0.093, 0.292)	(0.13, 0.004)	(0.005, 0.054)	(0.024, 0.015)
Always-off	(0.086, 0.454)	(0.084, 0.004)	(0.004, 0.042)	(0.022, 0.016)
Always-false	(0.168, 0.757)	(.165, 0.0022)	(0.0033, 0.053)	(0.026, 0.0184)
Non-malicious	(0.101, 0.536)	(0.097, 0.0033)	(0.0037, 0.04)	(0.017, 0.013)

compared with the fitted distribution to the expected trust user behaviour (as mentioned in Table 3.3). In the comparison, the Kullback-Leibler divergence (KLD) is used to analyze the difference in the probability distribution. KLD is a statistical measure which reveals how close a probability distribution to a candidate distribution [Shlens 2014]. As shown in Table 3.4 the attack behaviours and the expected non-malicious behaviour are presented. The standard error of approximation values are compared in Table 3.4. The standard error values are computed for each statistical measure (e.g. mean, variance) depending on the statistical distribution. Each statistical measure is indicated for the respective distribution in Table 3.4. Based on these results it can be concluded that standard error is minimum when the behaviours are approximated by a Weibull distribution with different values for the statistical measures. In order to compare with the context-dependent trust explained in [Qin et al. 2009], the standard error approximation for the Beta distribution is compared. Based on the standard error values, it is evident that the Beta distribution explains the attack models well but not better than the Weibull distribution.

The attack behaviours characterized by $MATM$ attributes are simulated as per Table 3.3 and the outcome is statistically approximated to a Beta distribution. Then, the equivalent parameters $P_{f,i} \equiv E1$ and $P_{m,i} \equiv E2$ [Qin et al. 2009] is used for the simulation. Outcome is statistically approximated to a Beta distribution. The fitted Beta distributions for each of the two distributions are compared. The KLD measure is used to estimate the

Table 3.5: Comparison of SSDF Attack Behaviour using $MATM$ and Context-dependent Trust [Qin et al. 2009]. α and β corresponds to the shape parameters of the Beta distribution using Kullback-Leibler divergence (KLD).

Attack Behaviour	Proposed Model		[Qin et al. 2009]		KLD
	α	β	α	β	
Always-on	2.38	5.71	2	3.71	0.0643
Always-off	1.74	7.31	2	3.71	0.4515
Always-false	3.18	13.7	2	3.71	0.5487

difference between the two distributions that are being compared (see Table 3.5). In the next experiment, the variation of the $MATM$ can be traced and used as a heuristic to identify the malicious behaviours of SSDF attackers.

The attack behaviours (Table 3.3) were simulated such that for each iteration any one of the above mentioned behaviours are randomly selected. Similarly, same number of iterations were run to compute the behaviours according to the equivalent parameters $P_{f,i} \equiv E1$ and $P_{m,i} \equiv E2$ [Qin et al. 2009] used for the simulation. The two sets of data generated from the two simulations run contain any of the three types of attackers as well as the non-malicious users which can be identified based on the respective behaviours. The objective of this experiment was to compare the classification accuracy of $MATM$ with the context-dependent trust metric [Qin et al. 2009]. The performance was analyzed using different classification techniques available in WEKA [Holmes et al. 1994]. Performance of the two models were compared using classification accuracy, false positive rate and true positive rate. According to the results (Table 3.7) it is evident that among the features and metrics used for reliable SU identification in the presence of SSDF attackers $MATM$ results in the most accurate identification. Using $MATM$, the average classification accuracy of 94.83% was obtained to distinctly identify the four classes. Therefore, it is more reliable to use $MATM$ for accurate non-malicious SU identification.

Next, the performance of genuine user selection accuracy of different cooperative user selection models are compared with the trust based methods described in [Hyder et al. 2014][Guo et al. 2015], context-dependent trust model [Qin et al. 2009], and [Feng et al. 2015] with $MATM$. Evidently, for $MATM$, it is possible to distinctly identify each of the three SSDF attacker classes with high accuracy.

Table 3.6: Classification Accuracy of *MATM* and Context-dependent Trust Model [Qin et al. 2009]. NB - Naive Bayes, MP - Multi-layer Perceptron, TP - True Positive, FP - False Positive, C1 - Always-on attacker class, C2 - Non-malicious User class, C3 - Always-off attacker class and C4 - Always-false attacker class.

Performace	*MATM* Model			[Qin et al. 2009]		
	J48	NB	MP	J48	NB	MP
Classification Accuracy	87.625%	100%	96.875%	77.125%	71.375%	72.75%
TP Rate (C1, C2, C3, C4)	(0.96, 0.775, 1,0.77)	(1,1,1,1)	(0.98, 0.925, 1, 0.97)	(1,1, 0.54, 0.05)	(1,1, 0.415, 0.44)	(0.995, 1, 0.415, 0.5)
FP Rate (C1, C2, C3, C4)	(0.007, 0.075, 0, 0.077)	(0,0,0,0)	(0, 0.01, 0.022, 0.01)	(0.002, 0, 0.15, 0.153)	(0,0, 0.187, 0.195)	(0,0, 0.168, 0.19)

Table 3.7: Classification Accuracy of *MATM* and Context-dependent Trust Model [Qin et al. 2009], . NB - Naive Bayes, MP - Multi-layer Perceptron, TP - True Positive, FP - False Positive.

Model	No. of classes	Average FP rate (J48,NB,MP)	Average TP rate (J48,NB,MP)
[Hyder et al. 2014]	02	(0.9,0.9,0.85)	(0.14,0.2,0.13)
[Guo et al. 2015]	02	(0.82,0.78,0.8)	(0.2,0.23,0.26)
[Feng et al. 2015]	02	(0.7,0.7,0.78)	(0.32,0.3,0.3)
[Qin et al. 2009]	04	(0.64,0.7,0.73)	(0.09,0.098,0.09)
MATM model	04	(0.86,1,0.97)	(0.077,0,0.12)

3.6.2 Effect of Trusted Coalition Selection

The objective of this set of experiments is to show the effectiveness of *MATM* to compute the trustworthiness of a SU and to select the *TC*. *Example:* Consider a short-range TCRM application, such as precision agriculture referenced environment monitoring [Wang et al. 2006], time-critical health monitoring [Pantelopoulos and Bourbakis 2010], where the signal strength degradation due to fading is assumed to be a minimum. The experiment starts when the FC requests for the local sensing information from the SUs. It is assumed that the sensing capability of SUs follow the Gaussian distribution. For each SU, its true sensing capability is modeled by a Gaussian distribution with mean 0.6 and variance 0.2 [Wang et al. 2016a]. The reported sensing capability for a malicious SU is set to a high value of 0.95. The initial trust score for all nodes is set to 1 representing ignorance. Sens-

ing time is fixed to $20ms$. The signal-to-noise is set to $-2dB$. In the experiment there are 10 channels and 16 SUs. Location for each SU is predefined as a two dimensional Cartesian coordinate (in a 20×20 grid) and FC is placed at $(10, 10)$. Each SU provides the local sensing decisions to the FC over 500 transactions and randomly request to access the vacant channels for data transmission. Among the 16 SUs, a maximum of 50% of them are malicious (i.e. can exhibit any of the three SSDF behaviours [Cai et al. 2014]). For each subsequent interaction, each of the three attributes are updated according to the Table 3.3. The local signal-to-noise ratio for energy detection for each SU is taken from the data published in [Quan et al. 2008]. It is assumed that in each interaction with the FC, a SU will provide the following information, $E_{residual}$, X_j and acknowledgments sent by each SU to keep track of $D_{rsp,j}$. Based on these information provided by each SU, it is assumed that the FC keeps record of X_j, X_{total}, $D_{rsp,j}$ for each j^{th} SU and a record of $Resp_j$ for each SU. When the SUs send requests to access a vacant channel and based on whether those requests are granted and utilized the corresponding a_j and r_j information for each SU is also stored at the FC. Then, based on the recorded data the three trust attributes (A_1, A_2, A_3) for each of the SUs are computed. When the number of malicious users are increased the ratio between non-malicious (malicious) and total number user for $MATM$ based trust computation shows a decrement (increment). When the threshold to declare a trusted user is varied, the size of the TC varies. The results are shown in Figure 3.1.

As mentioned earlier, in this chapter the non-consensus based fusion rules are considered. Therefore, the trust based decision fusion scheme described in [Wang et al. 2016a] is not included in this comparison as it is proposed for consensus based decision fusion model. The accuracy of spectrum availability decision depends on both the selection of TC as well as the type of fusion rule. Performance of the cooperative spectrum sensing decision accuracy (in terms of Q_d and Q_f) for $MATM$ based TC selection for different fusion rules is comparatively analysed. The performance of the decision fusion when there is a TC selection versus random cooperative user selection is compared ($N = 8$). The experiment was conducted assuming energy detection and the decision fusion approximated using a Gaussian Q-function (G_Q) [Hu et al. 2013]. As evidenced by the results,

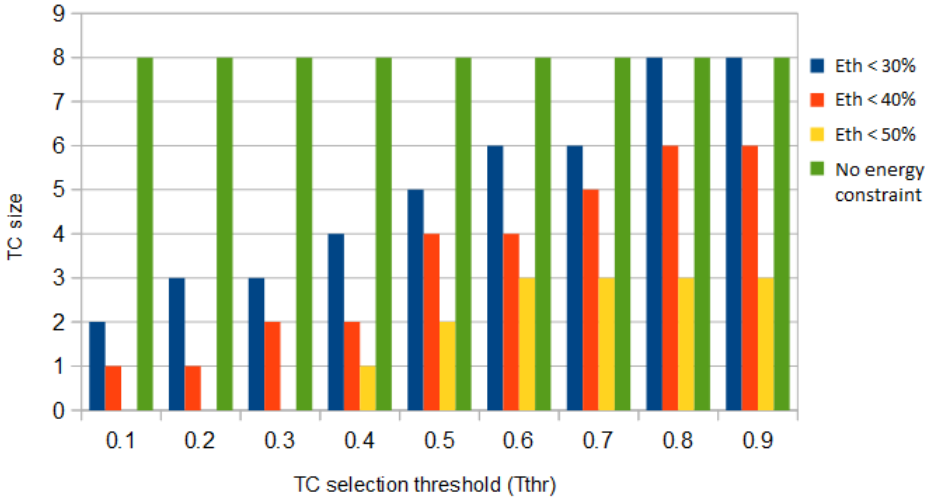


Figure 3.1: TC selection based on T_{thr} and E_{th}

the performance improves when there is a TC based decision fusion (Figures 3.2 and 3.3). Significant performance improvement is shown for AND rule as the final decision is 1 only when the sensing data are all 1. When there is a TC the performance improves. However, the size of the TC does not have a significant impact on the decision accuracy.

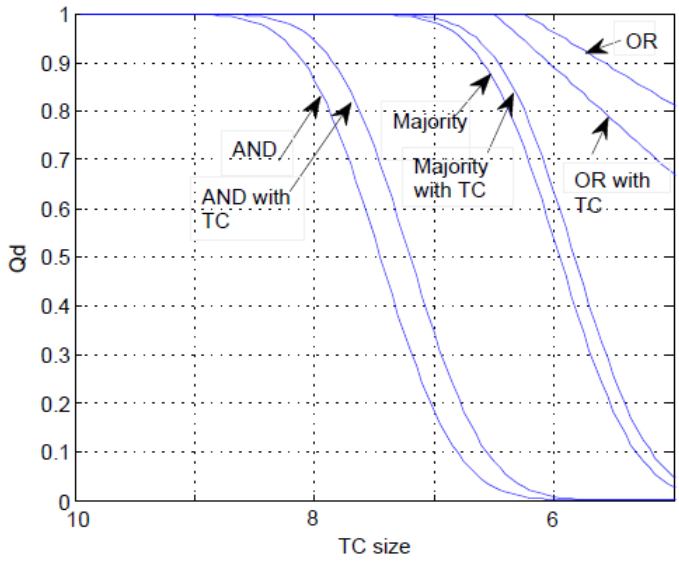


Figure 3.2: Variation of Q_d for Different Fusions Rules with TC Selection and Random User Selection.

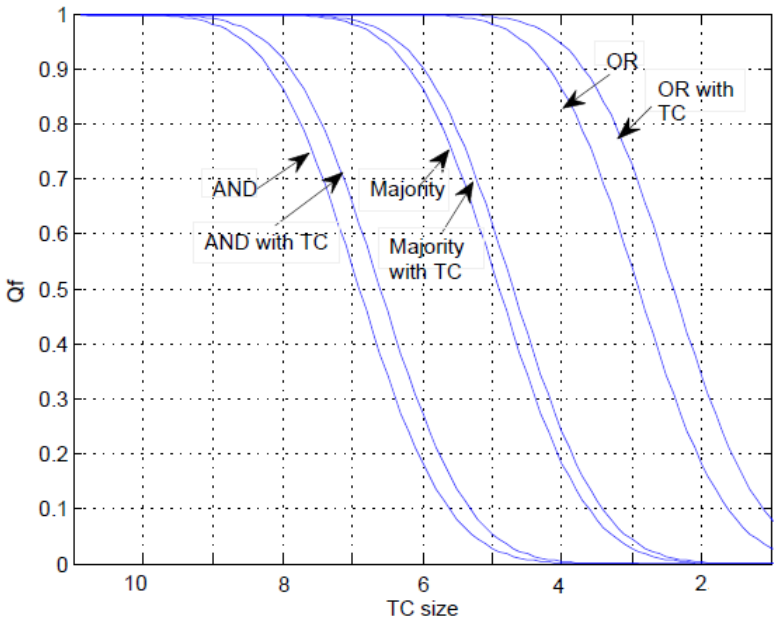


Figure 3.3: Variation of Q_f for Different Fusions Rules with TC Selection and Random User Selection.

3.6.3 Delay Analysis

In the proposed TC based cooperative spectrum sensing scheme, the secondary user transmission delay occurs in four cases: spectrum sensing, sensing results reporting, false alarm and correct detection of the PU. The delay caused by spectrum sensing and reporting is inevitable, since the cooperative SUs need to sense the spectrum and send the local sensing results to the FC to make a final decision on the PU status. To compute the delays in the latter two cases, the formulation used in [Hu et al. 2013] (the Equations 1 and 2 in [Hu et al. 2013]) is used where only a single sensing time slot is considered instead of multiple slots. For a single sensing time slot of duration τ, the $P_{f,j}(\lambda, \tau)$ and $P_{d,j}(\lambda, \tau)$ are computed as follows. In Equations 3.8 and 3.11 the associated sensing delays are incorporated. These are modified versions of the equations 1 and 2 in [Hu et al. 2013].

$$P_{f,j}(\lambda, \tau) = G_Q((\frac{\lambda}{var} - 1)\sqrt{\frac{\tau f_s}{2}}) \tag{3.8}$$

$$P_{d,j}(\lambda, \tau) = G_Q((\frac{\lambda}{var} - \gamma - 1)\sqrt{\frac{\tau f_s}{2}}) \tag{3.9}$$

The average delay for a SU is computed as (from Equation 3.10),

$$D(\tau, NR) = \tau + NR.t_r + (T - \tau + NR.t_r) \cdots \tag{3.10}$$
$$\times [p(h0)Q_f(\bar{\tau}, NR) + p(h1)Q_d(\bar{\tau}, NR)]$$

where,

$$\bar{Q_f} = \sum_{j=1}^{NR} \binom{NR}{l} P_{f,j}^{j}(\lambda, \tau)(1 - P_{f,j}^{NR-j}(\lambda, \tau)) \tag{3.11}$$

$$\bar{Q_d} = \sum_{i=1}^{NR} \binom{NR}{l} P_{d,j}^{j}(\lambda, \tau)(1 - P_{d,j}^{NR-j}(\lambda, \tau)) \tag{3.12}$$

For a frame duration of $T = 200ms$, the prior probability of the absence of a PU is taken as $p(h0) = 0.7$ which implies $p(h1) = 0.3$, $NR = 8$. A channel with a bandwidth of $1000Hz$ using binary phase shift keying modulation and noise of equal bandwidth is represented using a Gaussian variable with zero mean and var variance, $\lambda = 0.8$, the sensing time $\tau = 40ms$ and assumed $t_r = 0.5 * \tau$ for evaluation purposes. γ is varied between $2dB$ to $8dB$. Variation of the average delay with the signal-to-noise ratio is shown in Figure 3.4.

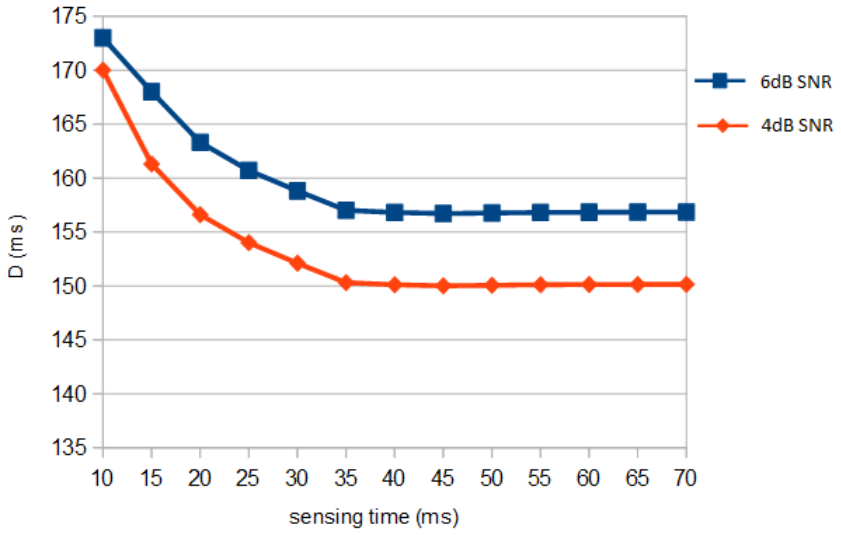


Figure 3.4: Variation of the delay with the spectrum sensing time for fixed $NR = 8$ and different γ values.

3.7 Conclusions

The main contributions of the chapter are, a novel multi-attribute trust attribute framework that is evidently shown to be useful for TCRM applications for i) user selection for cooperative spectrum sensing and ii) to identify the SSDF attackers distinctly based on the behaviours. The significance of these contributions enhances the overall reliability using cognitive radio networks for delay sensitive data transmissions in TCRMSs.

3.8 Epilogue

The next chapter investigates further improvements on delay bounded spectrum access when there are multiple interruptions due to primary user arrivals.

CHAPTER 4

Delay Sensitive Re-entrant Data Transmission

4.1 Outline of the Chapter

This chapter describes a reliable delay-sensitive persistent data transmission mechanism for TCRMSs provided that the available spectrum in the CRN has been accurately detected. The delay sensitive data transmission requires a cognitive sensing capable node to transmit data seamlessly within an acceptable delay when interrupted over multiple times due to the arrival of the PU on that channel. In order to ensure failure free transmission, an efficient hand-off management with a strict upper delay bound is necessary. The main contribution of this chapter is the delay bound computation for the re-entrants (i.e. the pre-empted SUs due to multiple interruptions) using the renewal counting process. The content of this chapter is under review.

The rest of the chapter is organized as follows. Section 4.2 provides an overview of the research problem, summary of the limitations of existing work and the specific contributions of the chapter. In Section 4.3, the notations used in this chapter are summarized. The re-entrant delay sensitive spectrum hand-off management approach is described in Section 4.4. In Section 4.5, the reliability of the delay sensitive analysis is described. Subsequently, in Section 4.6 experiments and the results are discussed. The chapter concludes with Section 4.7.

4.2 Introduction

When a SU is transmitting, it is not unlikely for a PU to arrive to start communications on that channel by interrupting the SU to pre-empt and vacate the channel [Sheikholeslami et al. 2015][Wang et al. 2012]. If the PU is co-existing in a channel, the SU does not get pre-empted [Nguyen et al. 2013]. Else, as the PU has a higher priority over the SU, then, SU gets pre-empted resulting in an interruption or a failure in its data transmission. Once a SU is interrupted, in order to complete the transmission of the remaining data, it is necessary to provide the re-entrant with another available channel or the same channel after a waiting for the PU to completed its transmission.

As mentioned in Chapter1, TCRMSs require the data to be transmitted over a period of time with minimal delay. In TCRMSs, when the transmissions are interrupted spectrum hand-off techniques are useful to access another available channel to continue the data transmission [Wang et al. 2010][Song and Xie 2012][Wang et al. 2012][Sheikholeslami et al. 2015]. However, when there are multiple interruptions over a period of time [Chai et al. 2014], the total transmission delay of a SU may increase due to spectrum hand-off. Evidently, if the sensing time is fixed and the collective cooperative spectrum availability decision making time is fixed, the contribution of waiting times for channel switching is significant for the total transmission time. Therefore, it is necessary to realize an effective mechanism for the SUs to re-gain transmission opportunities with spectrum hand-off management without exceeding a finite delay bound.

4.2.1 Limitations of Existing Work

In addition to the details on spectrum hand-off schemes described in Chapter 02, the always-staying and always-changing spectrum hand-off methods are discussed along with the existing re-entrant SU queuing models. Then, the scheduling methods suitable for queuing of the re-entrant SUs are discussed.

The IEEE 802.22 standard describes the listen-before-talk scheme in order to avoid causing harmful interferences to the PUs [Popescu et al. 2016]. When using a pre-emptive resume priority queuing model there can be two possible policies for spectrum hand-

off under the above contention-avoidance approach: (i) always-staying and (ii) always-changing [Wang et al. 2010][Wang et al. 2012]. In the always-staying policy, the SU will always stay in this channel until its data transmission is completed. In always-changing policy, the SU will switch to another channel when an interruption happens. For instance, if there is a target channel which is idle, the SU can execute data transmission immediately. Otherwise, the SU has to wait until a channel is idle.

For TCRMSs, it is necessary to ensure a likelihood of spectrum access in the next attempt without exceeding a pre-defined maximum tolerable delay. It is reasonable to assume atleast twice the active period of spectrum sensing as a tolerable delay limit for cognitive radio networks when the channel switching time during a hand-off is significantly small [Liu et al. 2013] (e.g. for $15s$ of active spectrum sensing time [Weichold et al. 2015], the maximum tolerable delay can be set as $30s$). In [Wang et al. 2012] multiple hand-offs resulting due to multiple interruptions have been studied. The authors propose a pre-emptive queuing model with proactive decision making to reduce the extended data delivery period considering different traffic arrival and service time distributions. The effects of multi-user sharing and multiple interruptions on the extended data delivery time of the SUs were also studied in [Borgonovo et al. 2008] [Shiang and Van der Schaar 2008]. The main limitation of the above solutions is the requirement for the secondary users to stay on the current operating channel to complete their unfinished transmissions. The waiting time is not limited based on a delay constraint. In [Zhang et al. 2013a], the authors describe a delay analysis of the re-entrants when there are multiple interruptions. In their experimental analysis the maximum number of interruptions are limited to 5. However, the maximum number of attempts within a given tolerable delay has not been considered. In [Wu et al. 2014], assignment of priority values during spectrum hand-offs based on the quality-of-experience for multimedia transmissions are discussed. When there are multiple interruptions, the channel with a maximum expected mean opinion score for spectrum hand-off is allocated in order to enhance the quality-of-experience. Based on the above discussion, although the multiple interruptions cause delays for data transmissions, the existing solutions do not consider the number of possible hand-offs permissible to satisfy a pre-defined maximum tolerable delay.

Another important aspect is how the re-entrants should to be scheduled to allocate the channels. Scheduling methods to queue the pre-emptive re-entrants include the earliest-deadline-first (EDF) [Liebeherr et al. 1996], least laxity first (LLF) [Mok 1983][Oh and Yang 1998], maximum urgency first (MUF) [Salmani et al. 2005] and modified least laxity first (MLLF) [Oh and Yang 1998]. Group priority EDF [Li and Ba 2012] is not considered as a suitable mechanism for pre-emptive scheduling due to the inability to ensure the different groups of re-entrants. In EDF, the priority is assigned based on the deadline. Earliest deadline gets higher priority than the late deadlines. Laxity is the difference between the deadline before which a task must be completed and the amount of computation remaining to be performed. Least laxity gets the higher priority than a higher laxity value. In modified laxity scheduling, when there is a tie, the current task completes as long as the deadline is not missed. The maximum urgency first scheduling is performed in two phases: EDF is used to sort the tasks and then use laxity to re-sort the tasks. Performance measures [Salmani et al. 2005][Li and Ba 2012] to compare the scheduling methods include the success ratio and the utilization [Salmani et al. 2005][Li and Ba 2012] of the system. Success ratio is computed by dividing the number of tasks completed successfully by the sum of the execution times of all tasks. In general, the utilization of the system is computed as the ratio between the sum of the execution times of all tasks which are ready before the time that the system is terminated and the time that the system is terminated.

4.2.2 Contribution of the Chapter

Main contribution of this chapter is a solution to achieve efficient and reliable spectrum hand-off management in TCRMSs to complete delay sensitive data transmission over a CRN without violating a pre-defined maximum tolerable delay. The delay-bounded maximum number of re-trials for a re-entrant SU is computed based on renewal counting process with immediate replacements. Results reveal significant improvement of reliability in terms of reducing the delay when the probability of interruption (p_i) is reasonably large (on average $0.1 \leq p_i \leq 0.6$)

The above mentioned contributions complements some of the recently published work addressing the spectrum hand-off management in CRNs.

In [Zhang et al. 2012], the secondary users are divided into two classes, class-1 (SU1) and class-2 (SU2) secondary users where SU1 has a higher priority compared to SU2 which in turn has a lower priority with respect to the PUs' to use the vacant channels opportunistically. The authors considers reactive-decision hand-off management for the SU1and SU2 using Markov transition model combined with the preemptive resume priority (PRP). The authors have investigated the effects of multiple hand-off delay using a queuing model with Poisson arrival and service time distributions and two separate servers for the normal and re-entrant users. In contrast to the contributions of this chapter, the solution in [Zhang et al. 2012], considers more than one type of high priority SUs. The pre-emption of a lower priority SU occur due to any of the high priority SU or PU. There is no maximum tolerable delay constraint considered in the analysis. Moreover, in [Zhang et al. 2012] authors do not consider the requirement that an interrupted SU needs to complete its transmission before a certain deadline. In this chapter, for a TCRM application, it is assumed that a SU is required to complete its transmission within a maximum tolerable delay in spite of multiple pre-emptive interruptions.

In [Bicen et al. 2015], the authors characterize the use of a dedicated CRN for frame transmission and assess the spectrum efficiency and hand-off performance analytically. The results reveal that the delay for a SU in the absence of a dedicated radio is the sum of the time periods of spectrum sensing after interruptions. When in the presence of a dedicated radio, the delay depends on the PU arrival rate, and sensing periods after interruptions. The contributions of this chapter significantly complements the work of [Bicen et al. 2015], the total delay when the SU has a maximum tolerable delay.

In [Rehmani et al. 2013], the authors propose channel selections based on maximum connectivity in multi-hop ad-hoc CRNs. Although there is a channel selection strategy, it differs from the contributions of this chapter as it does not account for the delay involved in the sequential channel sensing. In this chapter the delay associated with each interruption and the largest delay possible for a potential interruption when compared to a pre-defined maximum tolerable delay is computed.

In [Zhang and Yeo 2014], optimal sequential channel sensing based on the maximum residual time is computed. For each interrupted SU, the maximum residual time is computed and a channel which can sustain a transmission over this time is selected after spectrum sensing. The worst case delay will then be the sum of the sensing times for each channel. In this chapter, the residual delay when compared to a maximum tolerable delay after each interruption is computed. Then, the channel which is immediately available is selected to continue with the transmission.

In [Azarfar et al. 2016], buffering and switching medium access control protocols are comparatively analysed for the spectrum hand-off performance. When the packet length geometric distribution model, the delay analysis is similar for a service-repeat model where the entire packet must be retransmitted after each interruption. The delay due to re-transmissions and the residual time is accounted. The contributions of this chapter complements the solution described in [Azarfar et al. 2016] as it does not necessitate retransmissions but to complete the transmission of the remaining packets. Furthermore, in the proposed model the main focus is to adhere to the maximum tolerable delay to complete the transmission despite the multiple interruptions.

4.3 Notations

This section summarizes the notations used in this chapter.

Notation	Description
$Arr_i(t)$	data arrival process of the i^{th} SU
$B_i(t)$	backlog of the buffer of i^{th} SU at time t.
k_{intr}	number of interruptions
k_{Att}	number of re-trials
k_{ch}	number of channels
ch_j	channel state information of the j^{th} channel
$CA_{i,j}$	channel assignment of the i^{th} SU and the j^{th} channel
C_j	channel capacity of the j^{th} channel

N	number of retrials
T_{Att}	time duration for k_{Att} no. of re-trials
T_{ac}	actual transmission time
d_{fading}	delay due to fading
$d_{tr,i}$	delay for transmission at the i^{th} retrial
D_{avg}	average delay
t	time variable
D_{total}	total delay
X_n	inter-arrival time of the n^{th} retrial
$\frac{k_{att}(t)}{t}$	time average retrial rate over the time interval $(0, t]$
$E()$	expectation operator
$m_{at}(t)$	expected number of retries
M	stopping time
d_{tc}	truncated delay constant
$t_{sw,i}$	channel switching delay to the i^{th} channel
$E[T_{wait}]_i$	expected waiting time at the i^{th} channel
p_i	probability of interruption by the i^{th} interruption event
$E[T_{busy}]_j$	expected busy time at the j^{th} channel
y_h, y_l	occupancy of the high and low priority users respectively
Res_h, Res_l	residual time of the high and low priority users respectively
$serv_h, serv_l$	service time of the high and low priority users respectively
$\bar{w}$	average waiting time
$\bar{Res}$	average residual time
$\bar{serv}$	average service time

4.4 Reliable Context-Aware Spectrum Access for the Re-entrant Users

This section describes a novel solution which addresses the problem of sensed spectrum allocation to re-entrant SUs for delay-sensitive data transmissions in TCRMSs. The main objective of this solution is to allocate available spectrum to the re-entrant SUs who need to complete their data transmissions without violating a pre-defined delay constraint.

4.4.1 Overview and Assumptions

Spectrum hand-off management allocates the vacant channels for the re-entrant SUs to continue with the data transmission. To establish access to a vacant channel, it is assumed that the common control channel has sufficient coverage for all the SUs [Nguyen et al. 2013]. In order to maximize the data transmission opportunity of the re-entrant SUs, it is assumed that each SU can retry more than once to gain spectrum accessibility. It is also assumed that the number of attempts to resume the transmission should be limited by a pre-defined maximum tolerable delay. In addition, the following assumptions are made.

1. At any time, only one user can transmit its data over a channel.
2. To increase the accuracy of spectrum availability detection, cooperative sensing is used.
3. Centralized spectrum sharing entity makes the spectrum allocation decisions
4. Re-entrant SUs gain higher priority than the new arrival SUs at a particular channel.
5. The SUs are pre-empted from spectrum access due to lower priority than the PU and the PU is non co-existent.
6. The coverage of the common control channel is sufficiently large for all the SUs.
7. For a particular channel, the interference levels are at a minimum and the impact of the interference sources are at a minimum.

It is also considered that each SU (for example say the i^{th} SU) receives data according to an arrival process $Arr_i(t)$. It is assumed that each i^{th} SU needs to transmit data over multiple time slots. This is equivalent to a scenario of transmitting a large amount of data. Let $B_i(t)$ be the backlog in the local buffer of the i^{th} SU waiting to be transmitted. When k_{ch} number of channels are assigned for transmission, a finite amount of data is transmitted by the i^{th} SU. The buffer capacity is updated as,

$$B_i(t+1) = (B_i(t) - \sum_{j=1}^{k_{ch}} CA_{i,j}C_jS_j) + X_i(t) \tag{4.1}$$

where S_j is the channel state information ($S_j \in \{0,1\}$, where 1 is for vacant and 0 for occupied status), $CA_{i,j}$ is the channel assignment for the i^{th} SU (i.e. $CA_{i,j} \in \{0,1\}$) and C_j is the channel capacity.

4.4.2 Impact of Channel Fading Conditions

The channel capacity may vary depending on fading and the channel type. According to [Goldsmith and Varaiya 1997], for a time-varying channel, the capacity is computed by considering a finite set of values for signal-to-noise ratio or SNR (γ) and the received signal bandwidth (BW). The capacity of a fading channel is defined in [Goldsmith and Varaiya 1997] as follows,

$$\begin{aligned} C &= \int_{\gamma} C_{\gamma}.p(\gamma)d\gamma \\ &= \int_{\gamma} BW.log(1+\gamma).p(\gamma)d\gamma \end{aligned} \tag{4.2}$$

when $C_\gamma = BW.log(1+\gamma)$ for a time-invariant additive white Gaussian noise (AWGN) channel. The extent of fading is indicated by the Nakagami parameter m. When $m = 1$, the scenario is such that the channel is experiencing Rayleigh fading. When $m = \infty$ the channel experiences AWGN channel without fading. When m goes from 1 to 2, the severity of fading decreases [Goldsmith and Varaiya 1997]. The relationship between γ and m is such that for a finite vale j, such that, $j = 1, 2, \cdots, mM \in \mathbb{Z}$, $\gamma_j = \frac{j}{m} + \gamma_0$, where γ_0 is the cut-off SNR value to maintain an optimal level of power [Goldsmith and

Varaiya 1997]. When the fading level vary over the channel, the available channel capacity changes accordingly. The results are shown in Section 4.6.2.

When the channel experiences fading, the capacity is expected to reduce. The transmission time will then increase. The actual transmission time may increase causing a larger delay. However, this is an additional delay which is independent of the spectrum hand-off delay due to multiple interruptions.

4.4.3 Spectrum Hand-off Management with Multiple Re-tries using Renewal Counting Process

A renewal process is a generalized counting process with independent identical inter-arrival times [Leon-Garcia 2004]. A renewal counting process with finite expectation of the inter-arrival times satisfy the law of large numbers. Suppose there are finite number of chances for transmissions over a particular spectrum band during a period of time. This is equivalent to the number of component replacements over that particular time period with minimum channel switching delays. Therefore, it is appropriate to use the renewal counting process to determine the spectrum access probability for a re-entrant SU.

It is assumed that the d_{tc} is a pre-defined tolerable maximum delay for a particular time-critical application. For a particular channel, a SU is expected to transmit. It is assumed that over k_{Att} number of attempts, it is possible for a SU to gain spectrum accessibility depending on the vacant spectrum. The average delay is computed for k_{Att} number of re-tries (see Equation 4.3).

$$D_{avg} = \frac{\sum_{i=1}^{k_{Att}} d_{tr,i}}{k_{Att}} \tag{4.3}$$

where, $d_{tr,i} = t_{sw,i} + E[T_{wait}]_i$ with $t_{sw,i}$ is the switching time and $E[T_{wait}]_i$ is the expected waiting time at the queue of the i^{th} channel. It is assumed that the switching time is much smaller compared to the waiting time. To compute the sufficient number of attempts for transmissions to sustain network operations over a finite time t, the Wald's equation [Wald 1944] and the elementary renewal theorem [Cox 1962] are used. The objective of this formulation is to compute an upper and a lower bound for the time

average renewal rate over the expected delay to gain spectrum access for time-critical data transmissions. Assume the number of finite attempts as $m_{at}(t)$ and it is denoted as a function of time. The event of a re-try for another available channel can take place only if the delay constraint is not violated. The maximum tolerable delay in an individual attempt is limited by a truncating constant d_{tc}. This requirement helps to formulate the inter-arrivals of the attempts as follows (Equation 4.4).

$$X_j^{d_{tc}} = d_{tc} \iff X_j \geq d_{tc} \tag{4.4}$$

Next, the spectrum access rate is computed using the Wald's equation [Wald 1944] and the elementary counting process. According to the Wald's equation [Wald 1944], a proven result exists as $E(\sum_{i=1}^{M}) = E(X1)E(M)$ where M is the stopping time and $E(X1)$ is the time to occur the first interruption event. Then, given that $0 < t < d_{tc} \leq T_{Att}$, using the Wald's equation [Wald 1944] the rate of spectrum access is computed as follows.

$$\frac{m_{at}(t)}{t} \leq \frac{1}{\mu^{d_{tc}}} + \frac{(d_{tc} - \mu^{d_{tc}})}{\mu^{d_{tc}} * t} \quad \text{where} \quad d_{tc} = \text{max. tolerable delay} \tag{4.5}$$

when $E(X_1^{d_{tc}}) = \mu^{d_{tc}}$ then Equation 4.5 evaluates to

$$\frac{m_{at}(t)}{t} \leq \frac{1}{\mu^{d_{tc}}} \quad \Rightarrow \quad (\frac{m_{at}(t)}{t})_{min} = \frac{1}{X_1^{d_{tc}}} \tag{4.6}$$

Therefore, Equation 4.6 is the minimum rate for a given value of d_{tc}. It can also be inferred that for any other value for d_{tc} (which satisfies $d_{tc} \leq X_j^{d_{tc}}$), the rate will be greater than the minimum (Equation 4.6). Once the re-entrant SU exceeds the delay (i.e. $T_{Att} = d_{tc}$), the spectrum sensing needs to start again to regain the channel access as a new arrival. After each re-try the total delay gets updated and the condition $\sum_{j}^{i-1} d_{tr,j} < d_{tc}$ is verified.

4.4.4 Delay Computations for Always-staying Spectrum Access Sequence

As mentioned in Section 4.2.1, there are two types of spectrum hand-off sequences: *always-staying* and *always-changing*. Continuing with the Equation 4.1, for *always-staying* se-

quence, the delay D_{avg} experienced over k_{intr} number of interruptions can be computed using the busy period (T_{busy}) (as the equivalent waiting time) due to the current high priority occupancy of a channel and the probability of being interrupted (p_i) during the i^{th} event of interruption (Equation 4.7).

$$D_{avg}.k_{intr} = (\sum_{i=1}^{k_{intr}} (E[T_{busy}]_j)(1-p_i) + \bar{t_{sw,i}}) \prod_{i=0}^{k_{intr}-1} p_i \tag{4.7}$$

Applying Little's formula, $E[T_{busy}]_j$ for the j^{th} channel can be computed using the relationship for a single server that the ratio between the busy period and the sum of both the idle and busy periods equal to the fraction of the time the server is busy. When there is a maximum tolerant delay for each retrial after experiencing an interruption, the Equation 4.7 can be re-written in terms of d' as shown in Equation 4.8. It is assumed that the maximum delay is experienced at each retrial over k_{intr} interruptions (i.e. $D_{avg} = d'$).

$$d' = \frac{(\sum_{i=1}^{k_{intr}} (E[T_{busy}]_j)(1-p_j) + \bar{t_{sw,i}}) \prod_{i=0}^{k_{intr}-1} p_i}{k_{intr}} \tag{4.8}$$

4.4.5 Delay Computations for Always-changing Spectrum Access Sequence

Similarly, total delay for *always-changing* hand-off sequence (Equation 4.9) depends on the expected waiting time ($E[T_{wait}]_j$) due to the current service time of the high priority occupancy in the j^{th} channel. According to the Little's formula, the waiting time is computed as the mean number of customers in the queue divided by the mean rate of arrivals. It can be assumed that the channel switching time is very small compared to the expected waiting time for a SU.

$$d' = \frac{(\sum_{j=1}^{k_{intr}} (E[T_{wait}]_j)(1-p_j) + \bar{t_{sw,j}}) \prod_{i=0}^{k_{intr}-1} p_i}{k_{intr}} \tag{4.9}$$

$E[T_{wait}]_j$ depends on the residual service time for the current high priority occupancy and the cumulative work-load experienced due to the additional PU arrivals during T_{wait} in the j^{th} channel.

As mentioned in the previous section, the re-entrants need to be scheduled along with the remaining SUs for channel assignment. Once the schedule is prepared, spectrum allocation can be performed. For example, the Hungarian method [Kuhn 2010] is a well known method for allocating the channels. In the Hungarian method [Kuhn 2010] can find the optimal number of assignment of SUs to available primary channels, such that no two channels get assigned to one user and no two users get the same channel assigned. The scope of this chapter does not cover the spectrum allocation, but, assumes that for a TCRM application, channel allocation is reliable and efficient.

4.5 Reliability Analysis

In this section reliability analysis is performed to demonstrate the worst case delay for a re-entrant SU. It is assumed that the re-entrant SUs have a higher priority than the new arrival SUs to transmit on a particular channel.

When the spectrum is not available for a re-entrant SU it is a disadvantage as the opportunity to transmit is lost. This scenario can also be interpreted as degrading the high priority to a low priority. Therefore, it is reasonable to assume that two SU classes have equal priority. In such a scenario, the re-entrant priority class SU must wait for i) any high priority SU already in the queue, ii) any low priority SU already in the queue and iii) its own service time. Similarly, for a low priority SU there are three terms for the residual time. This can be summarized as follows (see Equation 4.10).

$$\bar{Res}_h = \bar{y_h} se\bar{r}v_h + \bar{y_l} se\bar{r}v_l + se\bar{r}v_h \tag{4.10}$$

$$\bar{Res}_l = \bar{y_h} se\bar{r}v_h + \bar{y_l} se\bar{r}v_l + se\bar{r}v_l \tag{4.11}$$

where Res_h and Res_l represent the residual times for high and low priority SU classes, $serv_h$ and $serv_l$ are the SU service times, y_h and y_l are the occupancy values. Since the waiting time is $\bar{w} = (\bar{Res} - se\bar{r}v)$, following results are obtained.

$$\bar{w_h} = \bar{w_l} = \bar{U_h}\bar{Res}_h + \bar{U_l}\bar{Res}_l \tag{4.12}$$

where U_h and U_l represents the fraction of time the server is busy with high and low priority class SUs. This result tells us that irrespective of the context, a fixed amount of waiting time is experienced by a SU. Considering the transmission during a time-slot, the value of $d' = \bar{w_h}$ computed using Equation 4.12 is the worst case waiting time for a re-entrant SU who intended to transmit during this time slot. For any other scenario the waiting time is less than $d' > \bar{w_h}$.

4.6 Experimental Analysis - Retrial based Scheduling

This section described the experiments conducted to evaluate the reliability of the proposed model and the effectiveness of scheduling the re-entrant SUs.

4.6.1 Experimental Setup

The re-entrant scheduling was simulated using Matlab Simulink with pre-defined delay constraints. The queuing model and the spectrum allocation strategies (both always-staying and always-changing access sequences) were implemented using the SimEvent library. The service time is an exponential distribution and the arrivals to follow a Poisson distribution. The maximum occupancy of the queue is varied and delay performance is compared. The main objective of the experiments were to demonstrate the feasibility of the proposed model and its effectiveness in adapting to different delay constraints.

Scheduling methods are compared to identify the most suitable scheduling strategy to queue the re-entrants. As described in Section 4.2.1, Earliest-deadline-first, least laxity first, maximum urgency first, modified least laxity first scheduling methods are compared. The two performance measures success ratios and utilization [Salmani et al. 2005][Li and Ba 2012] of the system are used to compare the performance of each scheduling method.

4.6.2 Results and Discussion

As described in Section 4.4.2, the backlog depends on the new data ($X_i(t)$) and the available channel capacity (see Equation 4.1). the effect of fading on the available channel capacity and the backlog is shown in the following results (see Figure 4.1). This analysis

consider the variation of fading to be as described in [Goldsmith and Varaiya 1997] when $m = 1$ to $m = 2$. Based on the results, it is evident that when the fading intensity reduces the available channel capacity increases and results in decreasing the total backlog.

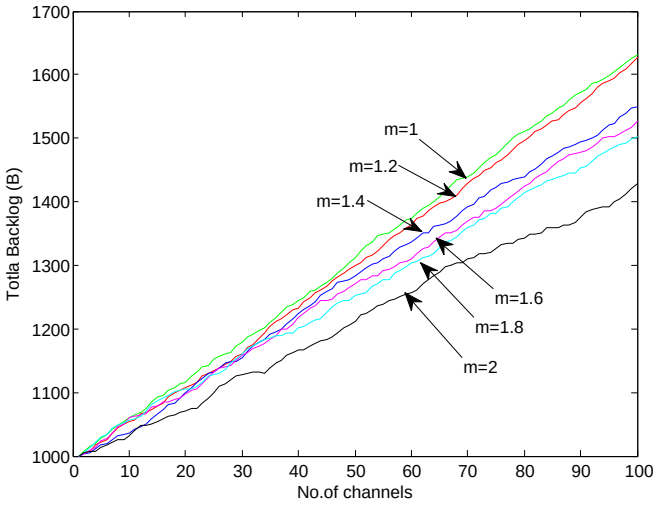


Figure 4.1: Effect of Fading on the available channel capacity (C) and the backlog (B) for a fixed new arrival data blocks.

As shown in Figure 4.2, the results of the re-entrant SUs and their retries for a single vacant channel in terms of delay constraints are described. In this particular simulation instance there are three retries and the corresponding inter-arrival pattern is shown in 4.2. Next, the variation of the number of re-entrants when there are more than one vacant channel and the corresponding average waiting time ($\bar{w}$) is shown in Figure 4.3.

As shown in Figure 4.4, variation of $d_{tr,i}$ is comparatively analysed for always-changing spectrum sequence based hand-off management. When p_i is a large value, $d_{tr,i}$ increases. When the service time takes an exponential distribution the impact of p_i to increase $d_{tr,i}$ reduces comparatively. However, the variation of $d_{tr,i}$ reduces for $0.1 \leq p_i \leq 0.5$ when the values of $d_{tr,i}$ increase as the number of re-trials (k_{Att}) increase up to nine (09).

As shown in Figure 4.5, when p_i increases, $d_{tr,i}$ also increase. Compared to a fixed T_{busy} value when it takes an exponential distribution, overall $d_{tr,i}$ is much lower in the latter case. It can also be inferred that when the number of re-trials are greater than six (06) the delay reduces for any $0.1 \leq p_i \leq 0.9$.

Comparing the delay variations in always-staying and always-changing spectrum se-

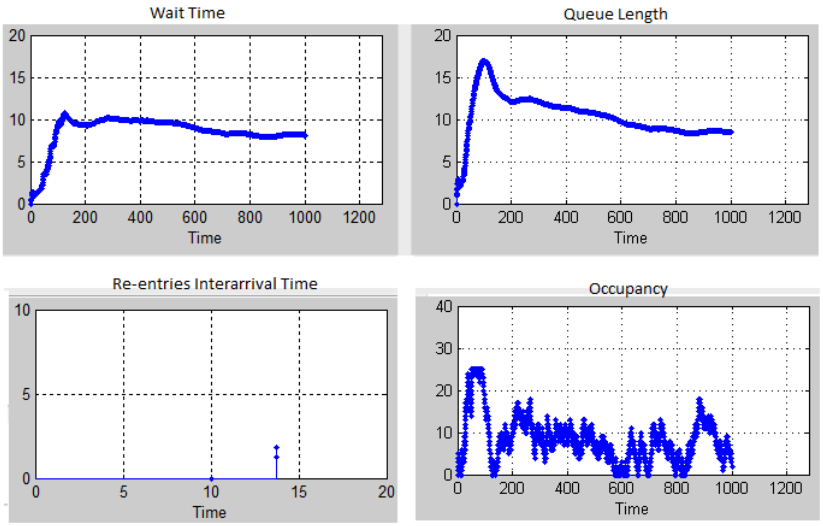


Figure 4.2: Simulation Experiment Scenario - The results of the reschedule of the high priority SUs in the priority based feedback queuing model with a single channel. In this particular scenario the blocking probability is 0. The maximum occupancy of the queue is 25.

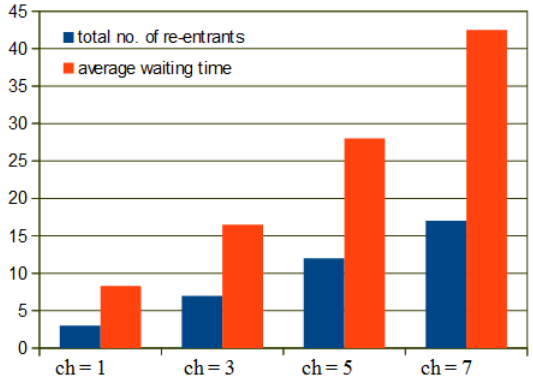


Figure 4.3: Variation of the total number of re-entrants and the average waiting time ($\bar{w}$) for different number of vacant channels.

quences for hand-off management, Following inferences can be made. First, it can be inferred that p_i is a significant factor which contributes to high $d_{tr,i}$ values. Second, for always-changing spectrum sequences, delay relatively decreases for an exponential service time distribution. Third, when the number of retrials increase at different thresholds the EDF based scheduling policy becomes most effective as the delay reduces to zero.

Next, the average delay of the proposed delay sensitive re-trial method are compared.

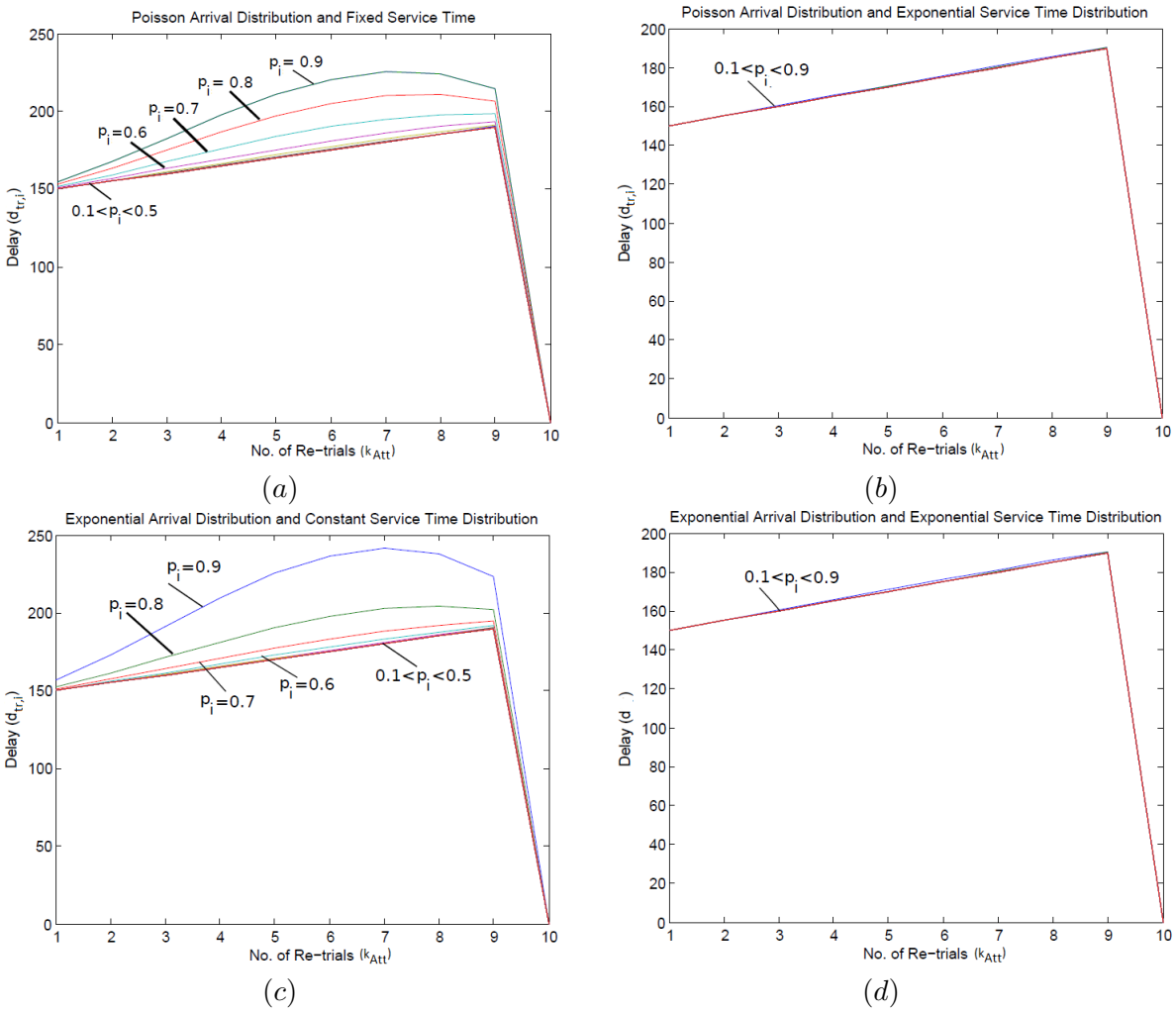


Figure 4.4: Delay ($d_{tr,i}$) analysis of Always-Changing Spectrum Access Sequence with the number of re-trials (k_{Att}). Results are shown for different arrival and service time distributions for different probabilities of being interrupted (p_i).

As mentioned before, [Zhang et al. 2013a] consider a maximum of 5 interruptions. In the experiment a single server pre-emptive priority queue with exponential arrival and service time is used. The occupants have priority labels assigned. Re-entrant SUs have a higher priority than the new SU arrivals. The PU has the highest priority. PU arrivals are random. Maximum tolerable delay of a SU is set as $d' = 30$ and the channel switching time is considered to be very small compared to the delay. The work of [Zhang et al. 2013a] and the proposed method are compared based on the expected delay for each user in a schedule with priority assigned users. In [Zhang et al. 2013a], the re-entrants are

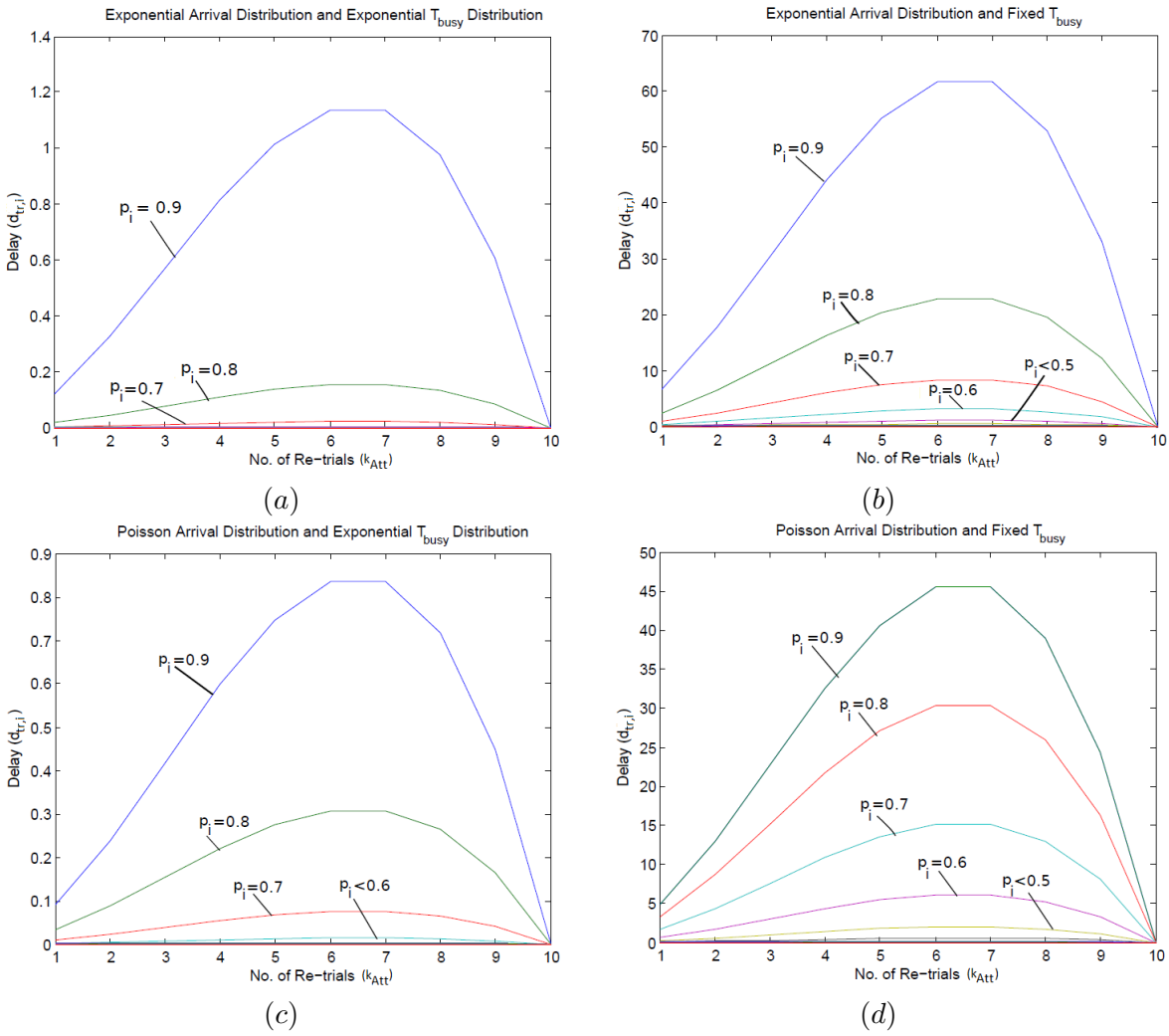


Figure 4.5: Delay ($d_{tr,i}$) analysis of Always-Staying Spectrum Access Sequence. Results are shown for different arrival and (T_{busy}) distributions for different probabilities of being interrupted (p_i).

not scheduled based on the delay but by a fixed higher priority than the new SUs in the queue. In the proposed method all the SUs are scheduled based on a pre-defined criterion (e.g. deadline, urgency).

Table 4.2: Comparison of Average Delay Variation when (i) the number of new SU arrivals are fixed (considered 06) and (ii) the number of new SU arrivals vary (each row corresponds to $6, 8, 10$ new SU arrivals)

Re-entrants	Average Delay (s) using the Proposed Method			
	For Re-entrant (i)	For New SUs (i)	For Re-entrant (ii)	For New SUs (ii)
3	16.8	58.2	16.8	58.2
5	28.2	70.1	28.2	72.8
7	42.5	84.5	42.5	104.2

Based on the results shown in Table 4.2, when the proposed delay-constrained method is used the delay experienced by the re-entrants increases when either the number of re-entrants increased or when the queue becomes larger with new SU arrivals.

Next, the performance of different scheduling methods are empirically assessed to identify which may offer the lowest possible delay for a re-entrant as well as for a newly arrived SU. In this experiment the maximum delay and the maximum execution time both are 100. Execution time are exponentially distributed with an expected value of 15. The time duration of a task is assigned from the range (maximum execution time, maximum delay) with a uniform probability distribution. Deadlines are assigned based on the time duration of that task. The average values of the performance measures are computed after 300 repeated experimental instances. Figure 4.6 shows the performance of the scheduling methods. Based on the results, MUF is more reliable for re-entrant scheduling as the success ratio is higher than the other three methods.

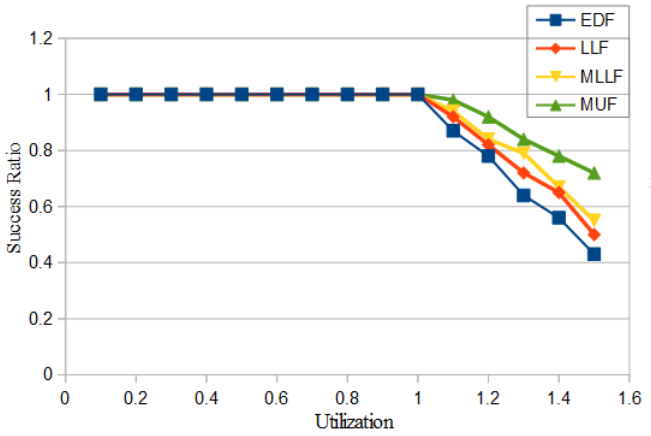


Figure 4.6: Comparison of Different Re-entrant Scheduling Methods (Earliest-deadline-first (EDF) [Liebeherr et al. 1996], least laxity first (LLF) [Mok 1983][Oh and Yang 1998], maximum urgency first (MUF) [Salmani et al. 2005] and modified least laxity first (MLLF) [Oh and Yang 1998]). Performance measures are success ratio and the utilization [Salmani et al. 2005][Li and Ba 2012].

4.7 Conclusion

The possible number of attempts within a known delay bound is computed using renewal counting process. The main assumption is that the maximum tolerable delay is set as twice the largest possible active spectrum sensing time [Liu et al. 2013], which is considered as $30s$ [Weichold et al. 2015]. For always-changing spectrum hand-off approach, when the probability of interruptions is high, the maximum number of retrials are limited to nine (09) when the maximum tolerable delay is set to $30s$ provided that the channel switching time is very small. For the same maximum tolerable delay, the always-staying hand-off approach can allow up to six (06) re-trials. When compared to the available scheduling methods, maximum urgency first method is more suitable to schedule the re-entrants to achieve a greater utilization.

4.8 Epilogue

So far the reliable channel availability is guaranteed by trust based cooperative sensing and delay bounded persistent channel availability over unreliable sensed spectrum. In the

next chapter an energy efficient secure and reliable data transmission solution is described.

CHAPTER 5

Energy-efficient Secure Data Transmission

5.1 Outline of the Chapter

This chapter describes a reliable and secure energy efficient sensor data transmission solution for TCRMSs. Encrypted data transmission offers greater security compared to raw data transmission over unreliable wireless channels which are susceptible to malicious attacks such as sniffing, data modification using relays. Since the cognitive radio sensors have limited energy reserves, efficient data encryption and route selection are significant aspects of reliable data transmissions. Security of the encryption depends on the key size. If the channel conditions do not vary drastically so that the energy required for spectrum sensing does not increase, then, the power consumption for data encryption will be proportionate with the key size. However, energy-efficient encryption key length should be such that it is less susceptible to reproduce (or guessing attacks). The main contribution of this chapter is an energy-aware physically unclonable function (PUF) based encryption key size selection criterion based on the residual energy of the CR sensor. Also, under given conditions, it is analysed how the encryption key size affect the energy consumption and its impact on the energy efficient route selection methods. Part of the content of this chapter is published in [Premarathne et al. 2015c].

Rest of the chapter is organized as follows. In Section 5.2 an overview of the research problem, summary of the limitations of existing work and the specific contributions are described. The notations used in this chapter are summarized in Section 5.3. Next, in Section 5.4, the energy-aware physical unclonable function based key size selection model is described and the experimental results are discussed. Subsequently the residual energy efficient route selection using different cost metrics is analyzed in Section 5.5 where the remaining energy content vary due to the selected encryption key size. Finally, the Section 5.6 concludes the chapter.

5.2 Introduction

Energy reserves of CR sensors are limited. Most of the energy is consumed during the data transmission, encryption and spectrum sensing. Typical capacity of a sensor battery is about 2.5Ah [Mainwaring et al. 2002]. In CR sensors, apart from spectrum sensing and encryption, large amount of energy is spent on data transmissions (about 20nAh to transmit a data packet, about 1.25nAh for radio listening and 8nAh to receive a packet [Mainwaring et al. 2002]). In TCRMSs, sensed data need to be securely and reliably transmitted over the wireless channels. For example, in pervasive health monitoring systems and smart grid surveillance applications, 128 bit encryption key generated based on the Advanced Encryption Standard is used to securely transmit the sensitive data over unreliable wireless channels [Pantelopoulos and Bourbakis 2010][Al Ameen et al. 2012]. To ensure the minimal chances for key reproducibility, the encryption should be sufficiently robust with appropriate length or key size. On the other hand, the operational life-span of a sensor (generally measured in hours) will reduce due to rapid energy dissipation if it continues to encrypt using large keys over many iterations. Specifically, it depends on the energy consumed per encryption function while transmitting a block of data.

In addition to secure data transmission, the reliability of the relaying path is also a vital aspect in TCRMSs. If the intermediate sensors do not have sufficient energy reserves to support the data transmission, the data needs to be re-transmitted over an alternative path with a higher delay or completely lost. This is a significant failure for a TCRMS.

Also, due to rapid energy depletion, the mean time to failure will increase [Rausand and Høyland 2004] causing to degrade the overall dependability of the TCRMSs [Rausand and Høyland 2004]. Furthermore, the stability of route selection is vital for TCRMSs. However, due to the heterogeneity of resources in CRNs, for the TCRM applications the direct adoption of the conventional routing mechanisms may result in poor performance. According to [Youssef et al. 2014], instability means one or more sensors in the route becomes unreachable. Assuming that PU interferences are at a minimum, the instability can largely be attributed due to the low residual energy of the CR sensor nodes. Therefore, the energy efficient path selection is another important aspect of reliable data transmissions in TCRMSs.

Based on the above discussion it is evident that the significance of selecting an encryption key of sufficient length with energy efficiency provide more reliable and secure data transmissions for TCRMSs. Therefore, to ensure the data is reliably delivered to the destination energy-efficient encryption and residual energy-aware route selection is vital.

5.2.1 Limitations of Existing Work

In addition to the discussions provided in Section 2.2.4 and Section 2.2.3, additional information on existing low power encryption solutions and limitations of related work are discussed.

PUF hardware use simple digital circuits that are easy to fabricate and consume less power which are suitable for sensors [Herder et al. 2014][Rostami et al. 2014]. PUF based keys are highly secure. These keys cannot be forged since the responses are generated with hardware inherent noise characteristics which are unclonable [Rührmair et al. 2010]. PUF based key generation essentially requires the keys to be generated so as to preserve the uniqueness among the keys. Although the entire key cannot be cloned by equivalent hardware circuits, part of the key may be guessed to reveal the possible combination. Recent work propose physical unclonable functions (PUFs) based secure key generation and deployment schemes for more reliable data transmissions in wireless sensor networks based TCRMSs [Selimis et al. 2011][Guajardo et al. 2008]. In Section 2.2.5, examples of

PUF based mutual authentication solutions for TCRM applications are discussed. Among different PUF based key generation techniques include arbiter PUF [Devadas et al. 2008], pattern matching based PUF key deployment using a trusted server [Paral and Devadas 2011], which is more viable for distributed authentication applications.

Pattern Matching Method - Recent work on pattern matching approaches uses Hamming distance metric to preserve the uniqueness of PUF based cryptographic keys [Paral and Devadas 2011]. In this approach, the challenges are not disclosed, but the response bits are kept public [Paral and Devadas 2011]. In PUF-based pattern matching key generation technique requires multiple streams to select the patterns. Then, the key is generated as a composition of the selected patterns. These patterns are substrings in a long stream of (noisy) PUF output bits. These substring indices are considered to be secret as they directly reveal the secret key. The patterns are stored as public helper data; other stream bits are not exposed. In order to reconstruct the key, the patterns are matched along their regenerated streams. The matching procedure is essentially to measure the Hamming distance [Paral and Devadas 2011]. Among the advantage of the pattern matching method, the complex error correction logic, such as Bose Chaudhuri Hocquenghem (BCH) decoders [Bose and Ray-Chaudhuri 1960], are not required. In addition, this method [Paral and Devadas 2011] is a more efficient and less complex technique suitable for real-time decision making applications in TCRMSs (e.g. smart grid surveillance). However, if the key length is not sufficiently long enough, the helper data can be used to reveal the secret key by hardware attacks as well as statistical predictive attacks. For example, in replay attacks, the helper data is maliciously used to reconstruct the original secret PUF key [Rostami et al. 2014]. Therefore, it is necessary to ensure that there is a minimal chance for an attacker to disclose part of the key or the whole key by ensuring that the key size is sufficiently large.

As discussed in Section 2.2.5, although considerable work exist on PUF based sensors very few have addressed the energy efficient encryption using PUF applicable to sensors. To the best of the knowledge there are no existing work to be directly related to this work on CR sensors with PUF based secure data transmission applications. Therefore, the proposed solution is compared with the related works of [Meguerdichian and Potkonjak

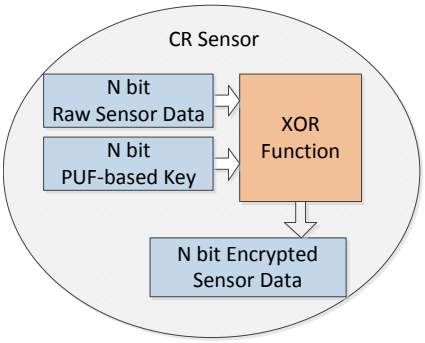


Figure 5.1: Block-Cipher Encryption Function in a Cognitive Radio (CR) Sensor. The encryption is equivalent to a one-way function with XOR operation over a data block with n-bit PUF-based secret key to output a ciphertext.

2011b] (M01) and [Wei and Potkonjak 2012] (M02) along with the energy aware routing protocols specifically recommended for CRNs [Youssef et al. 2014]. The two models M01 and M02 have been discussed in Section 2.2.5 and the energy aware routing protocols will be described in the next section.

5.2.2 Energy-aware Reliable Route Selection

Next, the energy aware route selection approaches are reviewed. Traditionally, multi-path routing refers to topology-wise disjoint paths with no common node except the source and the destination. This concept is useful in CRSNs to find spectrum-wise disjoint paths, based on a selected metric. These paths may share a common node [Youssef et al. 2014]. Another requirement for selecting such paths is that different bands/channels are assigned for the links around the common node [Youssef et al. 2014]. Among the various possible metrics, delay, route stability, energy efficiency are important concerns in TCRMSs. Several published work propose to use more than one metric and combine them as a global routing metric. For example, in [Ma et al. 2008] use routing metrics that combines channel switching time and multi-flow interference which contributes to the delay in transmission. As stated in [Herder et al. 2014], in order to achieve a performance trade-off among different routing metrics, these are combined to form a global metric. Among the available techniques which helps to combine different metrics include,

1. to form the global utility metric to combine the metrics in the form of weighted

Table 5.1: Existing Residual Energy based Cost Functions for Transmission Route Selection.

Cost Function ($C(rt)$)	Description
$e_{i,j}$	In [Ettus 1998] (M1), $e_{i,j}$ is the energy consumed to transmit one packet between i and j
$\frac{e_{i,j}}{E_i}$	In [Chang and Tassiulas 2004] (M2), $e_{i,j}$ is the energy consumed to transmit one packet between i and j, E_i is the residual energy at i
$\frac{e_{i,j}}{E_i^{tr}}$	In [Ok et al. 2009] (M3), $e_{i,j}$ is the energy consumed to transmit between i and j through tr, E_i is the residual energy at i
$exp(\frac{1}{sin(\pi-\frac{\pi E_i^{tr}}{E_0})})$	In [Liu et al. 2012] (M4), π is the period of the sine function, E_0 initial energy of i, E_i^{tr} current residual energy

exponential sum [Yu and Leitmann 1974].

2. to compute a lexicographic metric [Stadler 1988], in which the atomic routing metrics are arranged in the order of importance.

3. to compute a weighted min-max metric [Stadler 1988] to achieve certain balance and fairness among the different atomic metrics.

4. to transform each metric into constraints without introducing weights [Herder et al. 2014].

Existing energy efficient schemes for wireless sensors propose several measures to compare with the related work. In [Gandham et al. 2003], several comparable metrics for sensor life-time management are defined including the time for the first sensor to die, total number of messages received until a fraction of nodes die, energy spent in routing a message in one round. Additional metrics such as variation of node lifetime, average energy consumed per packet, time until the last node dies are proposed in [Younis et al. 2002]. However, these comparative measures are not specific for the PUF based solutions for sensors. Since this chapter focuses on the energy efficiency, the cost metrics based on the residual energy are considered. Summary of the existing transmission energy cost functions is shown in Table 5.1.

For a TCRM application, it is important to consider the cost of energy efficiency in terms of the residual energy to select a reliable path depending on data encryption

requirements. Since the primary stability concern for reliable data transmission is the residual energy of the CR sensors, recent review on CRN based route selection mechanisms have recommended the following protocols [Youssef et al. 2014]. In power aware routing protocol [Singh et al. 1998], there are five measures selected to ensure reliable energy aware route in an adhoc network. These five metrics are,(i) energy consumed per packet when transmitting over one hop, (ii) minimal set of nodes required to complete a reliable route, (iii) selection of node which have minimum number of packets waiting to be transmitted, (iv) residual energy of the sensor nodes and (v) total number of nodes (or the path length). In minimum weight routing protocol [Pyo and Hasegawa 2007], the cost of transmission between two points is stated in terms of the amount of transmission power computed using the free space propagation model. This solution consider the distance between the transmitter and receiver as the contributing factor. In NDM-AODV protocol [Ding and Liu 2010], the SUs are selected based on the residual energy. The total remaining energy is calculated for the path and then selects the path with the maximum value. All of the above recommended energy aware routing protocols for CRNs do not consider the contribution of encryption on the residual energy depletion.

5.2.3 Contributions

The main contributions of this chapter include the novel approach to select reliable and secure sensed data transmissions for TCRMSs. Specifically, the first contribution is to select the length of the encryption key such that minimum bit reproducibility is ensured. The Lovasz local lemma is used to compute the theoretical bounds on the minimal bit reproducibility of the PUF encryption key. The second contribution is the investigation of the impact of encryption key size selection on the energy aware path selection for reliable data transmission route selection.

To comparatively assess the contributions of this chapter with the related work described in Sections 2.2.5 and 2.2.4, four qualitative aspects are defined. The first qualitative aspect is the energy efficiency to support CR communications ($EECC$). It describes the extent of a particular solution to support energy efficient CR communications when

the PU interruptions are at a minimum and a large proportion of the energy is consumed for data transmission. The possible values are 1 and 0 which indicates the presence and absence of support for $EECC$ [Lee et al. 2013][Yang et al. 2011]. The second qualitative measure is the energy efficient secure key generation ($EESK$) is used to describe the ability of the solution to determine the PUF key size based on energy consumption of the CR sensor [Lin et al. 2010][Majzoobi et al. 2012]. The encryption key size is determined to adapt to the residual energy of the sensor rather than only to satisfy certain security requirements for data transmissions. The possible values are 1 and 0 which indicates the presence and absence of support for $EESK$.

The third aspect is the adaptive encryption key length selection to control minimum leakages ($AKCL$) [Herder et al. 2014][Devadas et al. 2008][Maes and Verbauwhede 2010] to ensure that the primary energy consumptions are dedicated to cognitive communications and PUF based security computations. The PUF based sensor solutions needs to prevent the power leakages to enhance its reliability by minimizing the key reproducibility. The possible values are 1 and 0 which indicates the presence and absence of support for $AKCL$. The forth aspect is the security against masquerading attacks ($SAMA$) [Delvaux and Verbauwhede 2014] [Meguerdichian and Potkonjak 2011a] [Lee et al. 2013]. It is the ability of the PUF solution provide sufficient resilience against tampering to launch masquerading attacks by exploiting the identity and location of a sensor. The possible values are 1 and 0 which indicates the presence and absence of support for $SAMA$.

Summary of the qualitative comparison is shown in Table 5.2. The subsequent sections will provide the detailed descriptions of the specific contributions.

Table 5.2: Qualitative Comparison with the Existing Work.

Existing Solution	*EECC*	*EESK*	*AKCL*	*SAMA*
[Meguerdichian and Potkonjak 2011b] - energy efficient PUF solution	0	0	0	1
[Wei and Potkonjak 2012] - lightweight PUF solution for wireless sensor networks	0	0	0	1
[Yang et al. 2011] - PUF authentications in delay tolerant wireless sensor networks	0	0	1	1
[Mahapatra et al. 2015] - PUF based mutual authentication	0	0	1	1
[Lee et al. 2013] - PUF based mutual authentication	0	0	1	1
[Meguerdichian and Potkonjak 2011b] - low energy mPPUF	0	0	1	1
[Delvaux and Verbauwhede 2014] - robust PUF based authentication	0	0	1	1
[Singh et al. 1998] - power aware routing	1	1	0	0
[Pyo and Hasegawa 2007] - minimum weight routing	1	1	0	0
[Ding and Liu 2010] - NDM-AODV routing	1	1	0	0
Proposed solution	1	1	1	1

5.3 Notations

In this section, the notations used in this chapter are summarized.

Notation	Description
k_{block}	block size (bits)
w_i	a bit pattern of the i^{th} key
sub_i	sub-string of a bit pattern of the i^{th} key
$P(Ev_i)$	probability of an event of reproducing a sub-string bit pattern
p	probability value ($p \in [0, 1]$)
oc	average probability of occurrence

$P(Ev_i^*)$	probability of non-existence of an event of reproducing a sub-string bit pattern
k_{ev}	total number of events
d	number of events which are mutually dependent to reproduce a key
Ev	set of all possible events
$G = (V, V_{ev})$	event dependency graph with V nodes and V_{ev} edges
$\bigcup$	union operator
$t_H d$	Hamming distance
R_{bit}	bit reproducibility
T_{Hd}	pre-defined threshold for Hamming distance
P_{miss}	probability of missing the reproducibility of a pattern
$P_{miss-bit}$	probability of missing the reproducibility of a bit
BIN	Binomial distribution
n	size of data (bits)
$z_{tr}(n)$	energy consumption to transmit an encrypted data block
$z_{pr}(n)$	energy consumption to encrypt a data block using a N bit encryption key
E^1_{total}	energy consumed during transmission of one bit
E^2_{total}	energy consumed during encryption of one bit
E_{total}	total energy expenditure in a CR sensor
$E_{residual,i}$	total residual energy after i rounds of data transmissions
E_0	initial residual energy before commencing the i rounds of data transmissions
$t1$	transmission time
$t2$	processing time
$t_{ch,idle}$	channel idle time
$P_{success}$	probability of most desirable channel transmission
d_{Rate}	data rate

N	encryption key size
op	the number of rounds of encryption per data block
$e(n)$	encryption efficiency
e_t	energy per bit consumed by the transmitter electronics
b	the energy dissipated in the transmit amplifier
$dist_{ij}$	the Euclidean distance between two nodes j and j
a_{pl}	the path loss factor
$k_{PU,act}$	the total number of instances which the PU was detected as active
k_{sense}	to the total number of spectrum sensing instances
$\bar{P_{intPU}}$	average probability of the potential PU interruption in a route rt
P_{intPU}	average probability of the potential PU interruption of a node
$C(rt)$	cost in terms of residual energy of the nodes in rt
$GM(rt)$	global route selection metric
ΔC	cost variation
ΔGM	variation in the global metric
ω	the relative weight set by the SU balancing the two atomic metrics indicating its preference
$EECC$	energy efficiency to support CR communications
$EESK$	energy efficient secure key generation
$AKCL$	adaptive encryption key length selection to control minimum leakages
$SAMA$	security against known masquerading attacks
DN	not applicable to address the feature requirement
PS	partially satisfying the feature requirement
FS	fully satisfying the feature requirement

5.4 Mutually Dependent Events for Pattern Reproducibility

In this section, the impact of pattern reproducibility with the PUF encryption key size is investigated. Novelty of this analysis is the use of Lovazs Local lemma to compute the mutually dependent event probability for pattern reproducibility [Paral and Devadas 2011].

It is generally assumed that for encrypting the data, the PUF-based secret key generation [Paral and Devadas 2011] and the raw sensor data are used. The encryption function is a bit-wise XOR operation over the blocks of size k_{block} bits (Figure 5.1). This approach is cryptographically strong, since a one-way compression function that transforms two fixed-length inputs into a fixed-length output, which makes it difficult, given a particular output, to compute inputs which compress to that output. The difficulty for pattern reproducibility of the PUF encryption depends on the size of the key.

5.4.1 Impact of Key Size on Pattern Reproducibility

It is evident, when the key size is large, the security offered is high as the reproducibility of the key reduces [Delvaux and Verbauwhede 2014][Paral and Devadas 2011]. However,for secure transmissions of CR sensors, large key sizes demand more processing power from the sensors in encrypting and decrypting the data since these devices have to perform spectrum sensing in addition to data transmission. Therefore, it is necessary to find a feasible pattern size to determine a sufficiently large key size based on the residual energy of the CR sensors.

Consider a pattern w_i which is vulnerable to be reproduced. The ability to predict the whole pattern w_i depends on the ability to guess the bit values based on an observed sub-string sub_i. This sub-string is part of the pattern w_i. This approach is more realistic than to assume independent guessing of each bit. The security objective is to reduce the likelihood of reproducibility of the patterns so as to minimize the misuse of PUF-based key generation. To address this requirement it is assumed that the events of guessing the

sub-strings of the pattern is not limited but the dependency of these events are limited. Such a dependency structure can be well represented by using the Lovasz local lemma [Moser and Tardos 2010]. In the Lovasz local lemma it states that, when the events are not independent of each other their dependencies can be restricted.

The probability of an event for reproducing a sub-string bit pattern is defined as $P(Ev_i) \leq p$ (where $0 < p < 1$). The probability of non-existence of an event with a dependency for reproducing a sub-string pattern is defined as $P(Ev_i^*) \geq 0$. If it is assumed that the dependent events occur very rarely, then, these event can be represented by Poisson trials. This is true only when the encryption key size is sufficiently large. Then, the value of $P(Ev_i) \approx e^{-oc}$ (where oc is the average probability of occurrence). Consider that the $P(Ev_i^*)$ is the probability of non-existence of an event of reproducing a sub-string bit pattern. In general, the aim is to prove that, the average event dependency probability is such that, $P(\cup_{j=1}^{d} Ev_j^*) = P(Ev_i | \cup_{j=1}^{d} Ev_j^* \leq P(Ev_i))$ where d is the number of such possible events with a mutual dependency.

In order to prove this result the event dependency graph structure is used [Moser and Tardos 2010]. Event dependency graph structure is $G = (V, V_{ev})$ such that $(Ev = Ev_1, \cdots, Ev_{k_{ev}})$ are the possible events to which $V = 1, \cdots, k_{ev}$ are the assigned numbers and $(i, j) \in V_{ev}$ (where i and j represents a number assigned to two nodes in the set V). An event Ev_i is mutually independent of the event Ev_j if $(i, j) \notin V_{ev}$.

The symmetric Lovasz local lemma states the following. Consider a set of 'bad' events Ev_i, which result in an undesirable outcome, in a probability space. Also, suppose each Ev_i is mutually independent of at least $n - (d + 1)$ other events and $P(Ev_i) \leq p$. If $e.p(d + 1) \leq 1$ (where $e = 2.718$), then, the probability $P(\cup_{j=1}^{d} Ev*_j) \geq 0$ is such that no bad event occur. In order to understand this result, p and d are evaluated for different combinations of values (Figure 5.2).

It is evident from the results that when the value of p is less, d increases. When the likelihood of an event occurrence is less the number of events which has a mutual dependency to reproduce a key increases. The implication is that the total possible event space has to be much larger. It is also interesting to see that the node degree increases when the probability $p < 0.3645$. So the range for $p = [0, 0.3645]$.

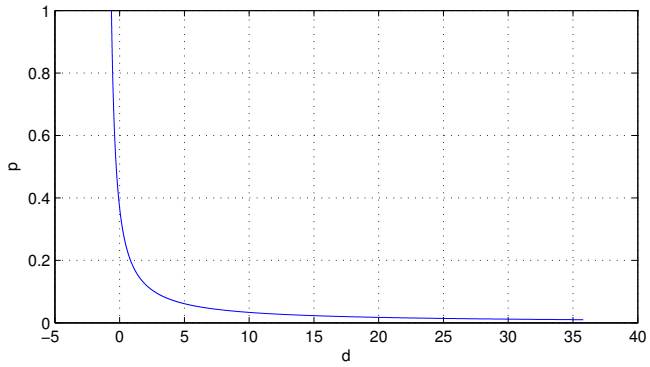


Figure 5.2: Relationship between p and d.

In [Delvaux and Verbauwhede 2014], for a pattern w_i, Hamming distance t_{Hd} (where a threshold value is defined as T_{Hd}), BIN is a Binomial distribution, and a bit reproducibility R_{bit}, the probability of missing the reproducibility of the pattern (P_{miss}) is defined as,

$$P_{miss} = 1 - \sum_{t_{Hd}=0}^{T_{Hd}} f_{BIN}(t; w_i, \bar{P_{miss-bit}}) \tag{5.1}$$

where, $P_{miss-bit} = 2R_{bit}(1 - R_{bit})$

$f_{BIN}(t; w, p) = (wt)p^t(i-p)^{w-t}$

$\bar{P_{miss-bit}} = \int_0^1 P_{miss-bit}(R_{bit}) PDF_{R_{bit}}(R_{bit}) dR_{bit}$

where $P_{miss-bit}$ is the probability of missing the reproducibility of a single bit. From the above formulation (see Equation 5.1, when $t_{Hd} = T_{Hd}$, the corresponding T_{Hd} values can be computed to satisfy the range for p. Different values for w_i were used for the analysis: $w_i = 8$, $w_i = 16$ and $w_i = 32$. Results are shown in Figures 5.3, 5.5 and 5.4 respectively.

The results for $w_i = 48$ and $w_i = 124$ are not shown as the values for p is very small in the order of 10^{-12}. Based on the results it is evident that when the key size grows the P_{miss} becomes very small as T_{Hd} can be a larger. However, in CR sensors, due to the residual energy constraints large keys may not be feasible to use for the data encryption. In such situations the $T_{Hd} = 3$ may take a low value for P_{miss} even when $P_{miss-bit}$ can

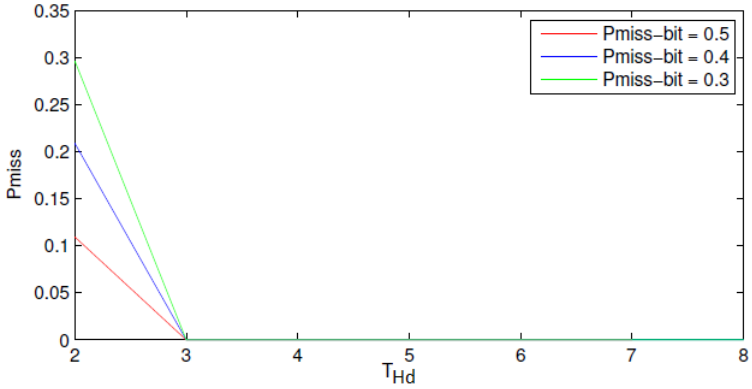


Figure 5.3: Relationship between T_{Hd} and P_{miss} when $w_i = 8$.

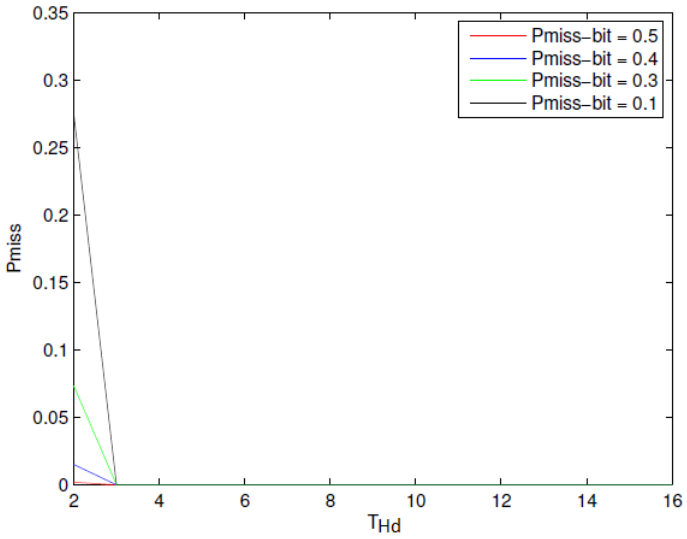


Figure 5.4: Relationship between T_{Hd} and P_{miss} when $w_i = 16$.

vary over a considerably wide range of value.

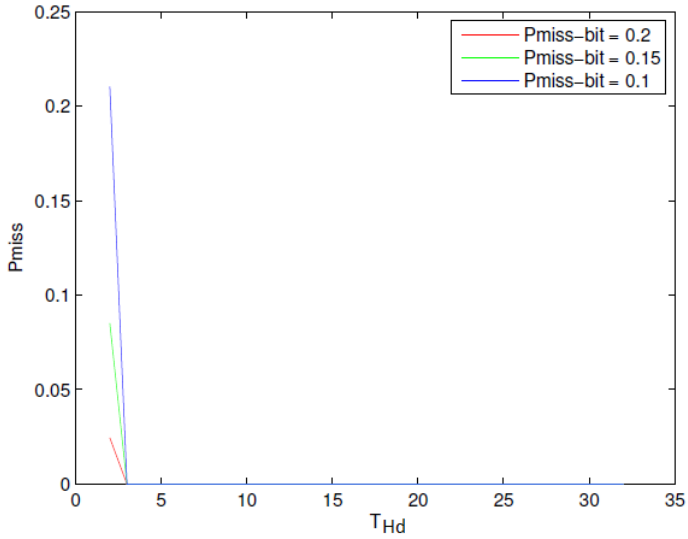


Figure 5.5: Relationship between T_{Hd} and P_{miss} when $w_i = 32$.

5.5 Residual Energy Constraint for Route Selection

In this section, the impact of the encryption key size on the residual energy based route selection is investigated.

5.5.1 Relationship between the Encryption Key and the Residual Energy

As mentioned in [Mainwaring et al. 2002], a typical sensor node (Mica sensor node) contains a AA battery of $2.5Ah(\approx 9000J)$. The total residual energy ($E_{residual,i}$) after i rounds of data transmissions depends on the initial energy content E_0 before the i rounds of data transmissions and the energy expenditure by each sensor $E_{exp,j}$, which in turn depends on z_{sense}: the percentage energy contribution for spectrum sensing, $z_{tr}(n)$ (Equation 5.3), and $z_{pr}(n)$ (Equation 5.4): the energy consumption in transmitting the encrypted data (of n bits) and the energy consumed in encrypting the data using N bit key respectively.

$$E_{residual,i} = E_0 - \sum_{j=1}^{i} E_{exp,j} \tag{5.2}$$
$$E_{exp,j} = (z_{tr}(n) + z_{pr}(n) + z_{sense})_j$$

$$z_{tr}(n) = E^1_{total}.P_{success}.n.t_1 \tag{5.3}$$

The transmission energy consumption for one bit is given in [Han et al. 2017] as $E^1_{total} = e_t + b \times dist_{ij}^{a_{pl}}$, where, e_t is the energy/bit consumed by the transmitter electronics, b is the energy dissipated in the transmit amplifier, $dist_{ij}$ is the Euclidean distance between two nodes i and j, and a_{pl} is the path loss factor. In [Mainwaring et al. 2002], it is stated that the energy consumption in electric circuit and the power amplifier of the transmitter circuit are in the order of nJ/bit and $pJ/bit/m^2$ respectively. In [Han et al. 2017], use $e_t = 50nJ/bit$, $b = 100pJ/bit/m^2$, $a_{pl} = 2$, $z_{sense} = 150nJ/bit$ and the $E_0 = 20J$ for a $500byte$ size packet over a $1kbps$ data rate for an AWGN channel with Rayleigh fading. t_1 is the transmission time and $P_{success} \in [0, 1]$ denotes the probability of the most desirable transmission channel state without any interruptions offered by the PUs and no collisions from SUs [Oto and Akan 2012].

$$z_{pr}(n) = E^2_{total}.e(n).t_2 \tag{5.4}$$

where E^2_{total} denotes the energy consumed during encryption of one bit, t_2 is the processing time to perform encryption $e(n)$ for n bits of data (in terms of number of computations Equation 5.5).

Since the proposed scheme is a symmetric encryption technique, it is assumed as a one-way block cipher computation with the transformation function as XOR (Figure 5.1). Based on the efficiency of a hash function stated in [Bartkewitz 2009], it can be approximated that the average computational efficiency of the encryption function as follows.

$$e(n) = \frac{op.n}{k_{block}} \tag{5.5}$$

where n is the size of the data chunk (i.e. total number of bits), op is the number of rounds of encryption per data block and k_{block} is the number of bits per data block. The value of op can also be considered as the product of the number of clock cycles [Kim et al. 2006] for each round and the number of rounds [Paral and Devadas 2011]. The block ciphers operate on a block of raw data with a fixed size and encrypt it using a symmetric key

where several modes of operations exist to encrypt large raw data chunks. For example, in counter mode, a nonce is combined with a counter value and encrypted. The result is used as encryption pad and XORed with the raw data. The XOR operation can be calculated in hardware in less than one clock cycle [Kleber et al. 2015]. For simplicity it is assumed that a XOR operation takes one clock cycle.

Next, consider the variation of the CR sensor energy expenditure for different encryption key size where the energy spent on transmission and spectrum sensing are considered to be constant. As shown in Figures 5.6 and 5.7, when the encryption key size is larger, the residual energy declines rapidly when compared to a smaller key size.

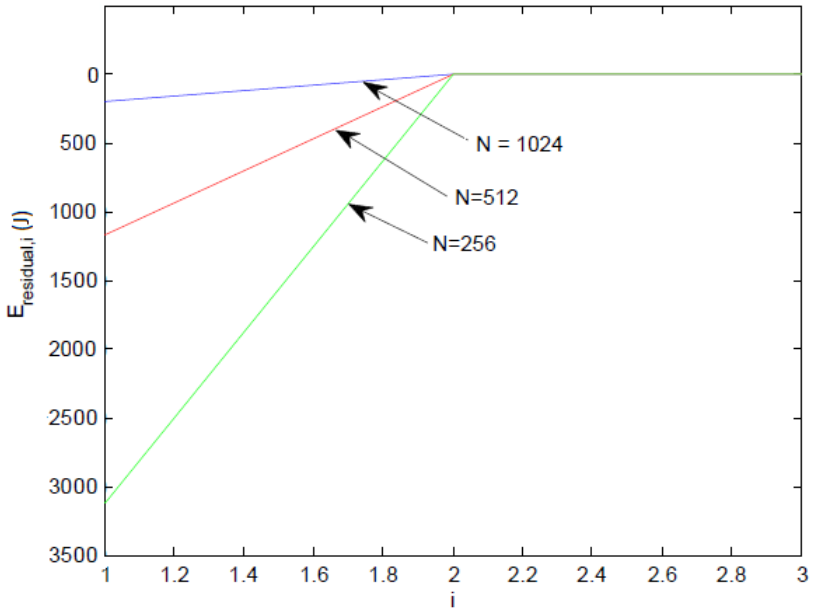


Figure 5.6: Variation of ($E_{residual,i}$) after i rounds of data transmissions for Different N values to transmit 1MB data with $E^2_{total} = 500nJ$.

5.5.2 Reliable Route Selection using Residual Energy Metric

In a CRN the path (or the route) through which the data are transmitted to a pre-defined destination is necessary. Multi-path routing is more focused here as it is more fault tolerant and thus more reliable. To select an appropriate route, among the several possible metrics [Herder et al. 2014], the link stability is vital. Shortest path is desirable for TCRMSs as the transmission delay will be a minimum.

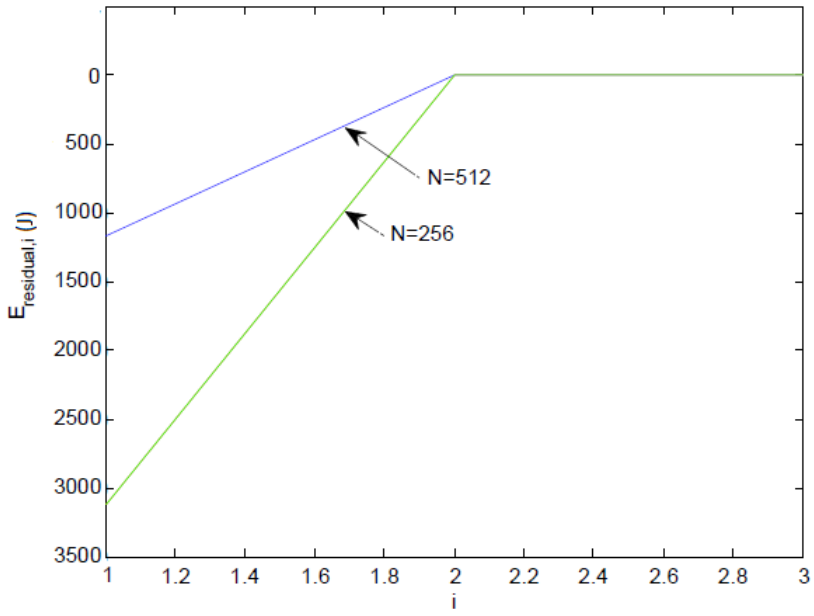


Figure 5.7: Variation of ($E_{residual,i}$) after i rounds of data transmissions for Different N values to transmit 1MB data with $E^2_{total} = 1000nJ$.

A more reliable route selection mechanism based on the residual energy and the likelihood of PU interruption is considered. Suppose the data is transmitted from a source to a destination, based on the minimum bit reproducibility requirement, the encryption key size is selected. Then, depending on the size of the data block the energy consumption is calculated assuming that the transmission power is fixed. Then, the residual energy of the transmitting node is computed. Once the source updates its residual energy to the FC, the most reliable path is selected based on the total residual energy of the other sensors along the shortest possible path.

Example : Consider the scenario in a smart grid surveillance application [Premarathne et al. 2015c], where, the CR nodes have to find the shortest path to reliable deliver the sensed data. In a potential shortest path (or a route rt), the stability of the link between two nodes depend on the (i) residual energy, and the (ii) likelihood of a PU interruption. It is assumed that the channel conditions do not vary drastically.

As the first metric, to assess the potential of a PU interruption, the PU activity history from the spectrum sensing data is used. As described in Chapter 01, the trustworthiness of a SU is vital to get more reliable spectrum sensing local decisions. Therefore, the trusted

SU data are used to compute the average probability of the potential PU interruption ($\bar{P_{intPU}}$) in a route rt. For each node, (P_{intPU})is computed as the ratio between the total number of instances which the PU was detected as active ($k_{PU,act}$) to the total number of spectrum sensing instances (k_{sense}). The link metric is computed as, $log(\bar{P_{intPU}})$ [Herder et al. 2014]. The second metric is the cost in terms of residual energy of the nodes, denoted as $C(rt)$. The link metric is the maximum total residual energy of the nodes in the route rt [Ding and Liu 2010]. In [Ding and Liu 2010], the number of possible routes is limited to 3. Next, to combine the two metrics into a global one, denoted as $GM(rt)$, weighted sum of exponentials method [Yu and Leitmann 1974] is used (Equation 5.6). This approach is compared with the linear combination method, where instead of the log value, ($\bar{P_{intPU}}$ is used in Equation 5.6.

$$GM(rt) = \omega.log(\bar{P_{intPU}}) + (1 - \omega).C(rt) \tag{5.6}$$

where ω is a relative weight set by the SU balancing the two atomic metrics indicating its preference. For example, smaller the value of ω, the SU prefers a greater stable and robust route less impacted by the PU traffic. When the cost variation is ΔC the corresponding variation in the global metric is ΔGM. It is evident from Figures 5.8 and 5.9, when the preference for the cost measure is high, the variation of the global metric is relatively small with a comparatively less increment as the $log(\bar{P_{intPU}})$ value increases. Thus, it is evident that in order to find the energy efficient route selection, it is a necessary condition to consider P_{intPU} to not have a drastic variation. In order to practically realize this requirement, the sufficient condition which needs to be satisfied becomes the accurate cooperative spectrum sensing ability of the CRN.

Next, existing transmission energy cost functions (shown in Table 5.1) are compared with the different PUF encryption key sizes provided that the minimum reproducibility is ensured with atleast $w_i > 32$ (see in Section 5.4.1). It is also assumed taht cooperative spectrum sensing is accurate and the P_{intPU} has a minimal impact on the reliability of route selection. Depending on the key size the selection of a route based on different residual energy dependent metrics (Table 5.1) is analyzed for a pre-defined network of

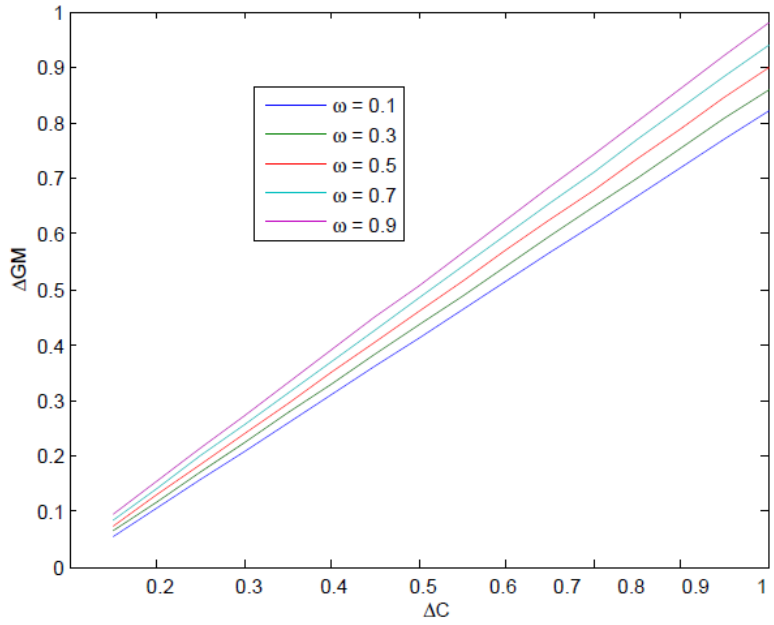


Figure 5.8: Linearly combined global metric variation ΔGM corresponding to the ΔC for different preference values (ω), where $0.1 < log(\bar{P_{intPU}}) < 1$ taken in ascending order with the corresponding ω.

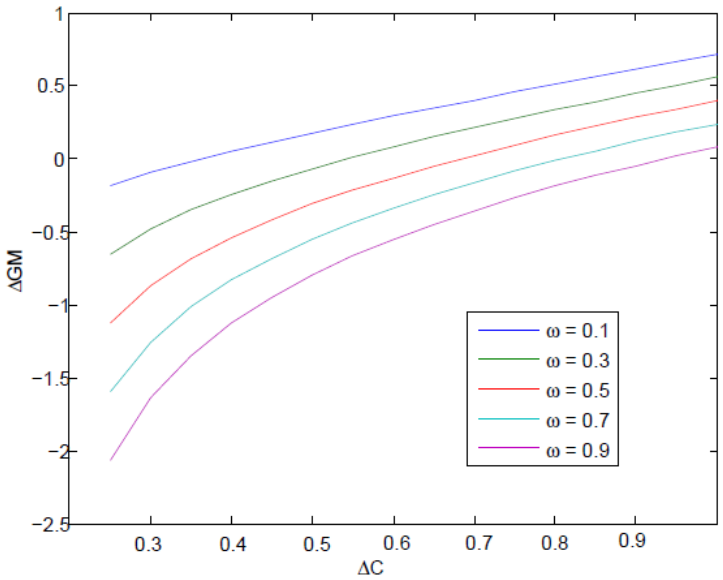


Figure 5.9: Global metric variation ΔGM based on weighted sum of exponential method [Yu and Leitmann 1974], corresponding to the ΔC for different preference values (ω), where $0.1 < log(\bar{P_{intPU}}) < 1$ taken in ascending order with the corresponding ω.

10 nodes (similar to the example shown in [Youssef et al. 2014]). As evidenced by the cost metrics shown in Table 5.4, the $rt1$ is more reliable based on the available energy to

Table 5.4: Residual energy based cost variation based on PUF encryption key size for routes $rt1$ and $rt2$ to transmit a 10kB packet.

Route	Key Size	Average value of $C(rt)$			
		M1	M2	M3	M4
rt1	1024	3.5J	0.45	0.287	0.167
	512	6.78J	0.7	0.56	3.164
	256	7.33J	0.7	0.758	0.3648
rt2	1024	2J	0.26	0.3	20.75
	512	4.5J	0.48	0.52	0.221
	256	6.2J	0.72	0.8	9.9018

transmit a packet of size 10kB.

5.6 Conclusion

This chapter describes an energy efficient key size selection method by ensuring minimum reproducibility of the encryption key for CR sensors. Based on the results, to produce a minimum reproducibility the pattern length should be 32 bits or a larger value. Furthermore, the impact of the encryption key size on the residual energy to select energy efficient paths for reliable data transmissions is analyzed. Based on the comparative analysis, performance of energy efficient route selection metrics reduces as the encryption consumes more energy due to large key sizes. Contributions of this chapter provides energy efficient secure and reliable data transmissions for TCRMSs.

5.7 Epilogue

The solution described in the next chapter helps to achieve reliable user authentications for data access using a trustworthy cloud based identity management model.

CHAPTER 6

Reliable Identity Management for Initial User Authentications

6.1 Outline of the Chapter

In TCRMSs, the sensed data stored in the cloud repositories are accessed by decision making agents to perform various decision making tasks. Authentication process is necessary to validate the claimed identity of a legitimate decision making agent based on a set of digital identities. Federated identity management is a scalable solution which effectively manage the digital identities in cloud platforms to facilitate the user authentications over trust negotiations. Inefficient user authentication mechanisms may require multiple iterations to validate the digital identities which result in significant delays to access the data. Furthermore, poor identity management with uncooperative and untrustworthy identity providers may cause prolong trust negotiations. Reliable identity provider identification is vital to ensure efficient failure-free user authentications in cloud data repositories of TCRMSs with federated identity management. The main contribution of this chapter includes the development of novel trust measures to assess the reliability of identity providers to facilitate efficient federated identity management. Part of the content of this chapter is published in [Premarathne et al. 2015a].

The rest of the chapter is organized as follows. In Section 6.2, the introduction to the research problem, limitations of the existing solutions and the contributions are described.

In Section 6.3, the notations used in this chapter are summarized. The significance of reliability and the related assumptions of the federated identity management system are discussed in Section 6.4. Next, in Section 6.5, novel trust metrics are defined. Subsequently, the experimental evaluations and the results are described in Sections 6.6 and 6.7. Finally, the chapter concludes with Section 6.8.

6.2 Introduction

Dependability of TCRMSs largely rely on the efficient decision making ability. This ability is determined based on how efficiently the sensed data can be accessed [Satyanarayanan et al. 2013]. Hindrance to access the remote monitoring data (e.g. continuous monitoring voltages at main breakers) may delay to process critical decisions (e.g. to operate a circuit breaker to stop a cascading failure in the smart grid) which may cause drastic consequences (e.g. black-outs). Access to data should only be granted to the legitimate users. User authentication is the main criteria to validate an incoming request initiated by a legitimate user. Authentication is a process in which a set of digital identities (or credentials) are validated to verify the claimed identity [Stallings 2006].

Cloud repositories are being used as scalable storage solutions to offer ubiquitous access to the sensed data generated from the distributed remote monitoring systems [Cummins 2017][Netbiter 2017]. In distributed computing platforms, between a user and a service provider, trust negotiations are used to authenticate the claimed identity of that user based on one or more digital identities [Bertino et al. 2010]. Trust negotiation is an iterative bilateral process in which an identity provider (e.g. the user or a trusted third party) discloses and exchanges the digital identities according to a set of pre-defined rules [Bertino et al. 2004]. The trust negotiations are advantageous as these are scalable and do not require complex access management policies to authenticate users. During a trust negotiation process, identity providers (IDPs) verify and provide necessary digital identities upon request from a service provider. Among the various identity management approaches used in cloud platforms, federated identity management is considered to be more appropriate to efficiently perform trust negotiations [Bertino et al. 2010][Noor

et al. 2013]. Failure to respond during a trust negotiation process may cause delays or a complete failure of authentication due to uncooperative identity providers. Thus, the reliability of a successful trust negotiation process to authenticate a user depends on the cooperation of identity providers in disclosing the appropriate digital identities.

In cloud computing, trust is used to describe the reliability of an entity (e.g. user, server, system component) in order to convince a service provider that an entity requesting to access data is accurately identified or credible [Nagarajan and Varadharajan 2011]. However, specific definition of trust depends on the application [Noor et al. 2013]. In this chapter, trust denotes the level of reliability of the identity providers expected by a particular service provider, in terms of their (i) cooperation in releasing the digital identities (or credentials) without prolonged delays and (ii) the ability to release digital identities (or credentials) without failure in view of potential security vulnerabilities.

6.2.1 Limitations of Existing Work

A detailed discussion of the trust management models in cloud environments has been given in [Noor et al. 2013]. Cloud based trust management models can be classified to four different categories: (i) policy, (ii) recommendations, (iii) reputation and (iv) prediction based. In policy based trust management a set of policies define a set of authorization levels with minimum trust thresholds [Noor et al. 2013]. The threshold trust values can be determined using, (a) monitoring and auditing approaches (e.g. service level agreement violations), (b) entity credibility approaches (e.g. response time, availability) or (c) feedback credibility (e.g. trustworthiness, expertise) approaches. Recommendations based models can use explicit or transitive recommendations [Krautheim et al. 2010]. Reputation based models compute aggregated trust metrics based on the feedback received by different users based on their previous interactions. Prediction based trust management models are used when there are no prior information regarding the cloud based interactions [Habib et al. 2013].

In general, for a particular entity, the history of successful interactions is determined when a non-conflicting service level policy (e.g. a service level agreement) is satisfied [Al-

mutairi et al. 2012] without considering any specific contextual requirements. Between two entities, the interaction history based trust is computed by taking the ratio between the number of successful interactions and the total number of interactions. It is important to note that its accuracy depends on the available information about the previous interactions between two entities. For example, to compute the trustworthiness of a service provider, the application specific interaction history is used to compute the context-dependent trust [Ries 2009]. In [Ries 2009], the context is measured in terms of the number of times a particular application is accessed. However, the intention of accessing the application, whether it is benign or malign, is not considered when computing this context-dependent trust.

Reputation based scoring techniques have been proposed to supplement the above mentioned information inadequacy of interaction history based trust [Jøsang et al. 2007]. Another solution to the information inadequacy is to use subjective logic [Jøsang et al. 2006][Cerutti et al. 2015]. In [Nagarajan and Varadharajan 2011], authors present a multiple trust attributes based framework and the trust attributes are combined using subjective logic.

In SelCSP [Ghosh et al. 2015], the service providers are selected using the trustworthiness and the competence. Using the trust and the competence level, a risk measure for a particular context: qualitatively stated in terms of importance and utility, is computed to rank the service providers. Competence is measured in terms of the conformance to the service level agreements. It is evaluated as {low (0.1), moderate (< 0.5), high (≥ 0.5)} with a score. Trust is computed based on the interaction history. When there are no previous interactions, reputation score is used. Trustworthiness is measured in terms of {distrusted (0 to 0.5), partially trusted (0.5 to 1.5), trusted (1.5 to 2)} with the corresponding scores.

In [Chahal and Singh 2016], service providers are selected based on public review trust, auditor trust and direct trust. The direct trust is computed based on the previous interaction history. Public review trust is computed based on the attributes: reliability, performance, security and vulnerability based on the information given by a broker (or a third party). Auditor trust is computed based on the attributes: performance, availability,

scalability and accuracy as monitored by an auditor. It is evident that the above mentioned trust based cloud service provider selection methods use additional trust measures other than the interaction history based direct trust.

In addition to the above mentioned solutions, computation of the trustworthiness of identity providers need to consider the security stealth against the existing security vulnerabilities to declare their responsiveness. This is significant for TCRMSs, where the contribution of a denial-of-service attack through malicious identity providers do not disrupt the access to the decision making agents [Li et al. 2012a][Niyato et al. 2013][Premarathne et al. 2015c].

6.2.2 Main Contributions

This chapter describes a set of novel trust attributes to assess the reliability of an identity provider to ensure a failure-free trust negotiation process to authenticate the users in a cloud platform. The main contribution of this chapter is a set of novel evidence-based trust attributes to evaluate the trustworthiness of identity providers. Computation of the metrics are based on the level of security enforcements, plausible attack resilience against selected security vulnerabilities and policy based constraints. Suitability of the proposed metrics is comparatively assessed using an existing cloud-based trust framework [Arias-Cabarcos et al. 2012b] for federated identity management. Results reveal that the proposed trust computation approach is more suitable to ensure a failure-free trust negotiation process for user authentications in TCRMSs.

6.3 Notations

This section summarizes the notations used in this chapter.

Notation	Description
IDP	identity provider
S	trust negotiation process
s_i	i^{th}step of the trust negotiation process

k_{tn}	number of steps in a trust negotiation process
$[DiscAttr]$	set of all possible identity credentials
$[\sigma]_i$	sub-set of identity credentials
$PL(X, Y)$	credential disclosure policy between a user X and a service provider Y
$P_{tr,j}$	probability of trust for carrying out an interaction when there is j^{th} security feature installed
k_{dsv}	known detectable and preventable security flaws in the absence of a security feature
k_{esv}	expected number of security vulnerabilities which requires atleast one particular security feature
$Y_{domain,i}$	number of domain specific policy dependencies in i^{th} sub-domain
$C_{domain,i}$	cost associated based on the complexity of evaluating the i^{th} domain specific policy dependent constraints
$Y_{sub-domain,i}$	number of sub-domain specific policy dependencies in i^{th} sub-domain
$C_{sub-domain,i}$	cost associated based on the complexity of evaluating the i^{th} sub-domain specific policy dependent constraints
S	trust negotiation process
s_i	i^{th} step of the trust negotiation process S
$P(s_i)$	the likelihood of credential disclosure in each step s_i
RA_j	risk attitude for the j^{th} attack scenario
N_{att}	number of attacks
pc	policy constraint
$[DiscAttr_{pc}]$	set of all possible credentials that can be disclosed by a particular policy pc
$[DiscAttr^*_{pc}]$	set of actually disclosed credentials based on a particular policy pc
dTN_{fu}	delay associated in gaining access to a service for a first time user
dTN_{ru}	delay associated in gaining access to a service for a recently serviced user

dTN^{w}_{fu}	worst-case delay associated in gaining access to a service for a first time user
dTN^{w}_{ru}	worst-case delay associated in gaining access to a service for a recently serviced user
dTN^{a}_{fu}	average-case delay associated in gaining access to a service for a first time user
dTN^{a}_{ru}	average-case delay associated in gaining access to a service for a recently serviced user
$min([dIDP_{s\_}])$	respective minimum value of the possible set of delays in the corresponding steps (i or j)

6.4 Overview of the Federated Identity Management Model

In this section the federated identity management model, the related requirements and the assumptions are described. Based on these requirements the novel trust metrics will be described in the next section.

In this thesis, it is assumed that the digital identities are managed using a federated identity management model in a cloud platform. There are four main entities in this identity management model (Figure 6.1): users, cloud service providers and identity providers. All these entities are assumed to have mutual trust relationships for reliable inter-communications. However, in order to reliably disclose the credentials, it is necessary to review the policy constraints [Yu et al. 2003]. In a more generalized scenario, in a cloud platform it is also possible for the user and a service provider to have their own policies of credential release and acceptance [Pearson and Casassa-Mont 2011][Ranchal et al. 2010]. It is assumed that the primary aspect of reliability of the identity providers is their cooperativeness in disclosing the digital identities of the users to ensure a failure-

free trust negotiation processes. According to the classification of identity management models described in [Zwattendorfer et al. 2013], it is possible for all of these entities to function as a single entity, or different entities, depending on whether they reside in the same domain or in different domains. In cloud platforms, a domain is a separable network which can be clearly identified using network identification measures including Internet protocol address, or virtual private network identities.

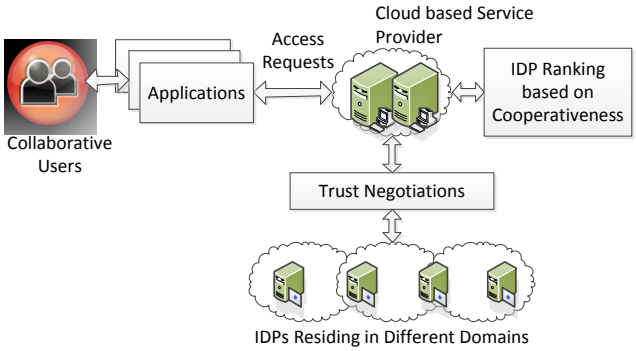


Figure 6.1: Functional Entities in Cloud based Trust Negotiations Model.

According to [Almutairi et al. 2012], the identity providers can collaborate as i) federated, ii) adhoc or iii) loosely coupled manner. In federated collaboration, the collaborating clouds are required to be managed through a global policy, which is consistent with their local policies. In a loosely coupled collaboration, there is no global policy but the local policies dominate. In the adhoc scenario, initially there are no restrictions to join or leave for collaboration. In this chapter, it is assumed that the identity providers collaborate in a loosely coupled manner so that the flexibility to authenticate a user through trust negotiations can be fully realized in the distributed network of a TCRMS.

According to [Almutairi et al. 2012][Gopalakrishnan 2009][Arias-Cabarcos et al. 2012a][Birrell and Schneider 2013], it is essential to consider the associated policies for credential disclosures in the respective domains in which the identity providers reside. These policies will state certain constraints involved during their communications over the trust negotiations [Baselice et al. 2007][Yu and Winslett 2003][Squicciarini et al. 2012]. For example, consider a set of credentials that is expected to be disclosed in a specific order. Generally, it is the underlying policy which will describe the order in which these are disclosed. For

example, whether the credentials are disclosed one after periodically the other or as tuples etc. Cooperative identity providers are assumed to adhere to these underlying policy constraints when releasing the credentials during a trust negotiation process.

6.4.1 Impact of Reliability of identity providers on Identity Disclosure in Federated Identity Management

Consider a trust negotiation process (S) with k_{tn} steps. The credentials disclosed at each step is a subset of all possible credentials $[DiscAttr]$ that can be disclosed.

$$[DiscAttr] = \{[\sigma_1], \cdots, [\sigma_{k_{tn}}]\} \tag{6.1}$$

where, $[\sigma_1] \cup [\sigma_2] \cup \cdots \cup [\sigma_{k_{tn}}] \subseteq [DiscAttr]$.

For example, assume for a trust negotiation step s_i is a tuple given by $s_i =< PL(X,Y), SP_1, SP_2, [\sigma]_i >$, where $PL(X,Y)$ is the credential disclosure policy between the user (X) and the service provider (Y) to disclose the credential $[\sigma]_i$ by an identity provider. The user X makes a data access request to a service provider Y. The user has a identity disclosure policy of $SP1$ and the service provider has a corresponding credential acceptance policy of $SP2$. To disclose the set of credentials $[\sigma]_i$, both the $SP1$ and $SP2$ should be non-conflicting. Then, the identity provider is able to disclose the credentials according to $PL(X,Y)$ between X and Y. The order in which the credentials are agreed to be disclosed should not be violated by the identity provider, as the order in which these are accepted by Y is non-conflicting.

Next, possible failures of credential disclosure strategies are analysed. First strategy, is where the credentials are disclosed *all-at-once*. Second strategy is the *step-by-step* credential disclosure over number of steps. At each step a finite number of credentials are disclosed. For the first strategy, for the response-to-request tuple (rs, rq), the failure criterion is stated as follows.

$$[DiscAttr^*_{pc}] \nsubseteq [DiscAttr_{pc}] \Leftrightarrow P(s_i) \neq 1 \tag{6.2}$$

where $([DiscAttr^*_{pc}] = [\sigma_1] \cup \cdots \cup [\sigma_i])$ is the set of actual credentials disclosed based on the known policy constraint pc and $[DiscAttr_{pc}]$ is the set of all possible credentials that

can be disclosed based on the same policy constraint. If $P(s_i) \neq 1$, then the likelihood of credential disclosure in each step s_i is unreliable since the pc is conflicting causing the trust negotiation process to fail.

For the second type of credential disclosure strategy, at each step s_i, a set of credentials ($[\sigma_i^*] \in [DiscAttr_{pc}]$) is disclosed. In order to preserve monotonicity of credential disclosure based on pc constraints [Yu et al. 2003], it implies that the identity providers should be cooperative. In order to satisfy the failure criterion, the identity providers should not be cooperative. If $[\sigma_i]$ is the set of credentials that is required to be disclosed during s_i in the negotiation process S, then the negotiations will fail if the disclosed credentials are not a subset of the intended credentials that requires to be disclosed.

$$[\sigma_i^*] \not\subseteq [\sigma_i] \Leftrightarrow P(s_i) \neq 1 \tag{6.3}$$

It is also possible to analyse the delays associated with the potential failures depending on the type of user. In general, for a cloud based federated identity management system, there can be two types of users: (i) first-time user, and (ii) a user who has been provided with the services recently [Bhargav-Spantzel et al. 2007][Gopalakrishnan 2009]. Consider a scenario which is similar to that described in [Bhargav-Spantzel et al. 2007]. An external user requesting a service for the first time requires to negotiate the necessary identity attributes from the identity providers. For a user, who has recently requested services, can easily retrieve the identity attributes from the respective identity providers in federation. This is possible based on their short-term session tickets and trust tickets. A trust ticket is issued at each step when the disclosure of the identities are successful where as a session ticket is issued for each trust negotiation process. If the delays associated in gaining access to a service for a first time user and a recently serviced user are dTN_{fu} and dTN_{ru} respectively, it is evident from the above discussion that $dTN_{fu} > dTN_{ru}$. These delays are solely due to the identity credential disclosures during the trust negotiation process assuming there is no other delays involved. However, if the identity providers do not cooperate and due to their untrustworthiness fail to disclose the required identity credentials, the trust negotiation process fail. In such a scenario, it is possible to compute

the worst-case delays (dTN^{w}_{fu} and dTN^{w}_{ru}) as follows.

$$dTN^{w}_{fu} = 2 * dTN_{fu} + \sum_{j} dIDP_{s_j} \tag{6.4}$$

$$dTN^{w}_{ru} = 2 * dTN_{ru} + \sum_{i} dIDP_{s_i} \tag{6.5}$$

For the average-case delay (dTN^{a}_{fu} and dTN^{a}_{ru}) for this scenario would then be computed as follows.

$$dTN^{a}_{fu} = 2 * dTN_{fu} + \min([dIDP_{s_j}]) \tag{6.6}$$

$$dTN^{a}_{ru} = 2 * dTN_{fu} + \min([dIDP_{s_i}]) \tag{6.7}$$

where $min([dIDP_{s\_}])$ indicate the respective minimum value of the possible set of delays in the corresponding steps (i or j) in the trust negotiation process. From the above formulation, it is evident that the largest delay contributing steps are most critical in determining the worst-case delay.

Based on the above discussion, in order to avoid the above mentioned failure conditions, the identity providers need to adhere to the *pc* constraints on the disclosure of the required credentials during the trust negotiation process S. Therefore, it is evident that in order to successfully complete a trust negotiation, the cooperativeness of the identity providers is vital.

6.5 Reliable Trust based Identity Provider Selection

In this section, the novel trust metrics are defined to rank the identity providers based on their reliability. The reliability is expressed collectively by these trust metrics. Then, the most reliable identity providers are selected when the collective trust value is higher than a pre-defined threshold.

6.5.1 Metric 01 - Security Threat Vulnerability based Trust

For an identity provider, greater exposure to vulnerabilities is an indication of more failure-prone unreliable disclosure of credentials. The risk attitudes can qualitatively describe the attitude of an identity provider to withstand the potential vulnerabilities despite

the installed security enforcements (e.g. firewalls, intrusion detection systems, network anomalous traffic filters). Different risk attitudes are useful to qualitatively compare the potential vulnerabilities [Weber 2010]. There are three different risk attitudes: (i) risk-averse, (ii) risk-loving and (iii) risk-neutral. Risk aversion is the dislike to take risks. Risk loving is the greater likelihood to take risks. Risk neutral means that there is no specific preference to like or dislike to take risks. A risk attitude is merely a descriptive label for the shape of a characteristic function [Weber and Milliman 1997] which describes how a risk factor behaves in a particular situation. In this chapter, the risk attitudes are used to describe each of the attack modeling factors [Schechter 2002][Schechter 2005]. In general, an attack is modeled using for four factors.

1. Risk to execute the attack (e.g. identity of the attacker being revealed),
2. Cost to execute the attack (e.g. time spent),
3. Rank of an adversary is determined based on the skills, tools used and the previous instances of attacks and
4. Incentives gained by the adversary by launching the attack.

The rank of an adversary and the potential incentives corresponds to risk-loving attitude. When the rank of the attacker is higher, it increases the likelihood of a successful attack. The cost and the risk of launching an attack corresponds to risk-averse attitude. For example, attackers are more likely to use less complex tools such as Extensible Markup Language - Denial of Service (X-DoS) due to lack of any real defense. On the other hand, risk loving attitude of the adversary describes the cost or the investment to succeed certain attacks. However, the time invested essentially increases the chances of an adversary being caught and identified which indicates that the risk factor is modeled as a risk averse behaviour. Incentives gained can be identified as a satisfaction (e.g. financial or psychological) gained by the attacker which takes a risk loving attitude.

For an identity provider, the value of $Metric01$ is computed as the average of the risk attitudes (RA_j) corresponding to the contributing attack modeling factors ($j = 1, 2, 3, 4, 5$) for N_{att} number of attacks (Equation 6.8). Larger value for $Metric01$ indicates that the

reliability of the identity provider is less while a lower value corresponds to higher reliability level.

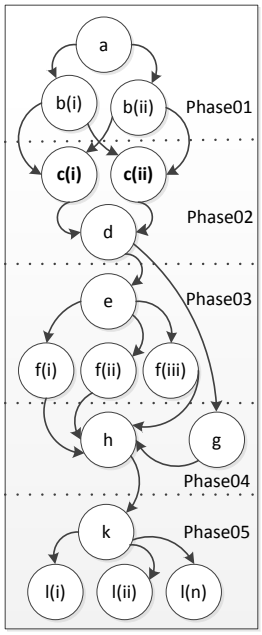
$$Metric01 = \frac{\sum_{N_{att}} \sum_{j} RA_j}{N_{att}} \tag{6.8}$$

Example: Consider the published data of distributed-denial-of-service (DDoS) attacks [in Cyber Systems and of MIT 2000]. The progress of a DDoS attack is a series of steps with specific malicious objectives (or outcomes). At each step the attacker aims to achieve a partial result. If all the steps are completed without failure, the attack is declared as successful which implies that the intended objectives (or incentives) of the attack have been achieved. Based on the data set 2000-1.0 of a DDOS attack data [in Cyber Systems and of MIT 2000] shows that the first phase of the attack contributes mostly to succeed the four subsequent phases (Figure 6.2). It is also evident that by just having resources do not assure the attack being successful. The perseverance and capabilities of an attacker also determines the success of an attack. The second 2000-2.0 DDoS attack data set, reveals that in the fifth phase of the attack, unless the attacker persist over several hours the attack may not succeed. Therefore, the rank of an adversary (modeled by the attack motive), the cost (modeled as resource consumption), benefits to the attacker and potential losses to the victim have to be considered when assessing the security threat vulnerability.

The novelty of trust computation using $Metric01$ is the application of risk attitudes to quantify the possible scenarios of loss of reliability of the identity providers corresponding to a known set of attacks. Each scenario is described using the above mentioned attack modeling factors. A fuzzy inference system is developed to determine the contribution of each of these four factors in order to compute the extent of the security threat vulnerability of an identity provider.

6.5.2 Metric 02 - Attack Resilient Strength based Trust

Although an identity provider is vulnerable, there may be security enforcements (e.g. firewall, traffic filters, intrusion detection systems) already installed to detect or mitigate



a – HINFO Query
b(i) – sadmind attack will work
b(ii) – correct stack pointer
c(i) – append user to a password file
c(ii) – append user to a shadow password file
d – sadmind attack breaks into Eyrie DNS server
e – ftp to mill
f(i) – break into Solaris host
f(ii) – break into mstream server
f(iii) – break into mstream master software
g – telnet to mill
h – launches script and break into Solaris hosts according to HINFO records
k – manually launch DDoS attack
l – attack each victim by flooding packets

Phase	Cost	Benefits	Loss	Rank
01	**Low**	**Very High**	**High**	High
02	Moderate	High	High	High
03	Moderate	Very High	High	High
04	High	High	High	High
05	***Very High***	High	***Low***	High

Figure 6.2: Data Set 1.0.2000 - A five phase DDoS Attack Scenario where the attacker probes the network, breaks in to a host by exploiting the Solaris sadmind vulnerability, installs trojan mstream DDoS software, and launches a DDoS attack at an off site server from the compromised host. Shows the dependency graph and the inferences over four features: Rank, Cost, Benefits and Loss.

certain types of attacks. In this view, the main limitations of using the $Metric01$ include the following.

- Require sufficient data to infer the necessary information on attack modeling factors and the associated risk types.
- Already implemented attack mitigation or preventive measures are not included in the trust computation.

To address the above limitations, the second trust measure is defined which uses the information about the security enforcements to mitigation strategies to assess the security stealth of an identity provider. For a particular security enforcement mechanism, three factors are considered to develop the $Metric02$.

- Number of threats that can be prevented,
- Number of threats that can be detected and

- Number of threats that cannot be prevented or detected by security enforcement mechanism.

For example, consider the firewall as the security enforcement. The firewall is expected to prevent as well as detect a set of known security threats [Wool 2004]. However, the understanding of the preventable and detectable security threats based on the actual operations can be less than the expected number. This difference may arise due to the new types of attacks or configuration errors [Wool 2004]. So if the level of security attributed to the firewall has to be computed, then, the ratio of known to expected preventable and detectable threats can be used. Based on these values the level of trust in terms of security resilience due to the firewall can be computed.

Next, the $Metric02$ computation for a particular identity provider is described. Probability of trust ($P_{tr,j}$) for carrying out a secure interaction due to the enforcement of a security feature $'j'$. For each security enforcement, it is computed as the ratio between the number of known preventable, detectable security flaws (k_{dsv}) and the expected number of security vulnerabilities (k_{esv}).

$$Metric02 = \sum_{j} P_{tr,j} = \sum_{j} (\frac{k_{dsv}}{k_{esv}}) \tag{6.9}$$

Practical limitation in accurately quantifying the k_{dsv} and k_{esv} for already available security enforcements, is the lack of sufficient information. Information about the vulnerabilities are publicly available on several databases such as Open Source Vulnerability Database (OSVDB), Common Vulnerabilities and Exposure List (CVE) and NIST National Vulnerability Database (NVD). In cloud computing platforms, the vendors and developers do not always provide comprehensive descriptions of all the possible preventable and detectable vulnerabilities along with the security enforcements. And also, over time there are new attacks and vulnerabilities discovered which makes it difficult to give an accurate prediction [Kohlrausch 2009][Grieco et al. 2016]. For example, zero-day attacks can be launched by exploiting vulnerabilities that has previously not been disclosed [Bilge and Dumitras 2012]. So unless potential vulnerabilities are known it is difficult to enforce countermeasures to completely detect and mitigate future attacks. In Section 6.6.2, to

compare the preventable and detectable set of attacks, the theory of fuzzy rough sets is used [Jensen and Shen 2002]. Any value less than 1 indicate the minimum security feature is enforced. When it is required to have more than one security feature, the security stealth measure may get interpreted as 'low' on a qualitative scale.

6.5.3 Policy Dependency based Cost Metric ($PDCM$)

The policy constraints are represented as a cost or an overhead [Almutairi et al. 2012][Gopalakrishnan 2009]. A cost based representation can assess the potential mis-trust contributed by an identity provider during a trust negotiation process. In this view, a policy dependency cost metric ($PDCM$) is defined as follows.

$$PDCM = \sum_{i=1} Y_{domain_i} . * C_{domain_i} + Y_{sub-domain_i} . * C_{sub-domain_i} \tag{6.10}$$

where Y_{domain_i} is the number of domain specific policy dependencies and C_{domain_i} is the associated cost estimated based on the level of complexity of evaluation. Similarly the number of sub-domains and the associated costs are denoted as $Y_{sub-domain_i}$ and $C_{sub-domain_i}$. A larger value for $PDCM$ indicates higher dependencies which lower the reliability for cooperation due to the dependency constraints.

In order to calculate the values for domain specific policy dependencies and the associated costs, service level agreement violations and the associated costs are used [Ullah et al. 2016]. Generally, the relationship between a cloud provider and a customer is governed with a Service Level Agreement (SLA). The SLA is established to define the level of the service and the associated costs. The failure of providing a service is called a SLA violation. To identify SLA violations it is necessary to have specific details of quality-of-service parameters and service level objectives (e.g. availability, throughput and response time). According to the recent publication [Ullah et al. 2016], provide the SLA violations and the corresponding costs. These published data are used for the $PDCM$ calculation (Table 6.3). According to the available data, there are no sub-domains involved in the SLA cost computation data.

Table 6.2: $PDCM$ Computation using Service Level Agreement Violations (no. of violations) and Associated Costs (monetary costs in terms of $) [Ullah et al. 2016].)

Identity Provider	Y_{domain}	C_{domain}	$PDCM$
$IDP01$	3184	97.21	3.091×10^5
$IDP02$	980	106.55	1.044×10^5
$IDP03$	1916	98.75	1.892×10^5
$IDP04$	464228	98.9	459.1×10^5
$IDP05$	47878	130.31	62.4×10^5
$IDP06$	53391	101.63	54.3×10^5
$IDP07$	59599	89.06	53.1×10^5
$IDP08$	327	95.29	0.312×10^5
$IDP09$	344	94.06	0.323×10^5
$IDP10$	36436	101.64	37.033×10^5

6.5.4 Trust based Ranking

The above described trust metrics ($Metric01$, $Metric02$ and $PDCM$) are used to estimate the reliability of the identity providers. The ranking process is essentially a two stage decision process. In the first stage the $PDCM$ values are computed. Then, overall trust is computed using $Metric01$ and $Metric02$. During the first decision making process, the identity providers with the lowest values for $PDCM$ are selected. During the second decision making process, from those selected identity providers, the ones with the largest overall trust values are selected to participate for the trust negotiations. Ranking of identity providers is demonstrated in the example described in Section 6.6.3.

6.6 Experiments and Results

In this section publicly available attack data and vulnerabilities are used to for the computations of the two trust metrics $Metric01$ and $Metric02$. Then, an example scenario is described to demonstrate the identity provider selection method based on $PDCM$.

6.6.1 Computation of $Metric01$

In order to compute the $Metric01$, attack history data sets are used [in Cyber Systems and of MIT 2000]. Specifically, the five (05) phase DDoS attack data sets (2000-1.0 (DS01) and 2000-2.0 (DS02)) of 2000 and two attack data sets of "mailbomb" (attack id - 42.155148) and "fdformat" (attack id - 52.16243504) of 1999 (DS03 and DS04 respectively) are used. For each attack scenario, the corresponding characteristic functions for the contributing attack modeling factors are derived. For example, according to the 1998 dataset the cost in terms of the time taken to launch the attack takes a numerical value. The risk, skill and the incentives take a qualitative value $\{high, moderate, low\}$. Then, the RA_j values are computed for each attack scenario. Fuzzy variables are able to model linguistic declarations such as low, medium, high, etc [Dondo 2008]. A fuzzy number is assigned with a range of possible values to represent each linguistic descriptors. To make inferences using these fuzzy numbers, if-then rules are specifically defined. To obtain the result of the inference, defuzzification process is applied to get the crisp values. In [Dondo 2008], a vulnerability is represented using a fuzzy number. To compute the $Metric01$, the attack modeling factors are assigned with the appropriate fuzzy numbers. Membership functions are selected and defined for each attribute depending on the range it needs to represent. The convention is to select a simple (i.e. less computationally complex) membership function to represent an attribute [Dondo 2008]. Examples of such simple membership functions include triangular, trapezoidal. In addition, the membership function should be able to adequately describe the range of possible values for each attribute.

By definition, the risk attitude is computed as the ratio between the first and the second derivative of the characteristic functional form, also known as the utility function [Arrow 1964][Millner and Pratt 1991][Weber and Milliman 1997]. On a normalized scale,

the utility of a risk attitude takes a maximum value of 1 and a minimum of 0. Generally, the risk averse attitude is described using concave utility functions [Keeney 1972]. Examples include the logarithmic and power functions. The risk loving attitude is described using convex utility functions. Examples include exponential and negative power functions. However, if there are not enough numerical data to support the attack modeling factors to characterize the utility functions, then, more flexible methods which can account for descriptive values (e.g. cost of the attack is high, low or moderate) need to be considered.

Table 6.3: Analysis of the Contributions of Each Attack Modeling Factor (Skill of the attacker, Cost to launch the attack (in terms of time) and the Incentives gained by the attacker.)

1998 Data Set [in Cyber Systems and of MIT 2000]			
Attack name	Skill	Cost	Incentives
back	low	high	high
dict	high	low	high
eject	low	high	high
ffb	high	high	high
format	low	moderate	high
ftp-write	moderate	low	high
guest	high	high	high
imap	moderate	low	high
ipsweep	low	high	high
land	high	high	high
loadmodule	high	high	high
multihop	high	moderate	high
neptune	high	high	high
nmap	low	moderate	high
perlmagic	high	high	high
phf	low	high	high

pod	low	high	high
portsweep	high	high	high
rootkit	high	high	high
satan	high	high	high
smurf	high	high	high
spy	high	high	high
syslog	high	high	high
teardrop	high	moderate	high
warez	high	high	high
warezclient	moderate	low	high
warezmaster	high	high	high
2000 Data Sets [in Cyber Systems and of MIT 2000]			
DDoS 2.0.2	low	high	low
DDoS 1.0	low	high	low
1999 Stealth Attack Data Set [in Cyber Systems and of MIT 2000]			
eject	high	moderate	high
sqlattack	high	moderate	high
loadmodule	high	moderate	high
ps	high	moderate	high
ffb	high	low	high
perl	high	low	high
format	high	low	high

Among the four attack modeling factors, the extent of the attackers' identity being revealed does not have sufficient data to be evaluated. Therefore, in this experiment only three attack modeling factors are considered. For example, 1998 data set [in Cyber Systems and of MIT 2000], the cost of launching the attacks in terms of the normalized time never falls below 0.33 or beyond 1. Low and moderate costs are differentiated around 0.43.

Between the high costs are distinguished from the moderate costs above 0.52. Attacker skill is qualitatively evaluated as follows: 0.7 and above as high, 0.5 and below 0.7 as moderate, between 0.3 and 0.5 as low [Kotenko and Doynikova 2014]. According to [Pardue et al. 2010], based on the simulation experiments, it is reasonable to value the attack incentives as follows: above 0.3 up to 1 as "High", between 0.2 to 0.3 as moderate and lowest possible being 0. Table 6.3 shows the summary of the analysis for an attack dataset. The output is the risk attitude (RA_j). As shown in Figure 6.3, low and moderate risk attitudes are represented using the psigmf function already defined in Matlab fuzzy inference toolbox (the shape represent the risk averse behaviour in separate interval) while the high RA_j value is represented using sigmf function defined in Matlab fuzzy inference toolbox (to describe a risk loving behaviour). Corresponding fuzzy inference output using the trapezoidal fuzzy membership functions is shown in Figure 6.4.

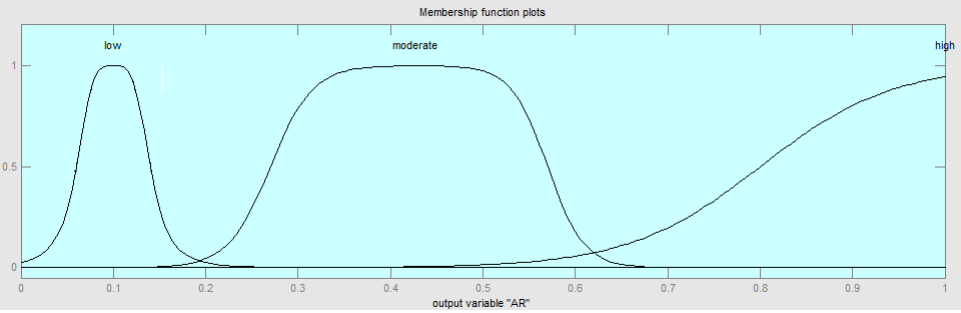


Figure 6.3: Memebership Functions to Represent RA for each attack modeling metric.

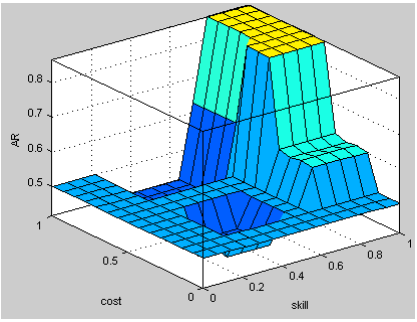


Figure 6.4: RA output for attacker skill factor and cost factor.

To demonstrate how the $Metric01$ is calculated, consider the following example scenario. Assume there are five identity providers. These identity providers are assumed to

be vulnerable to a set of security threats (from Table 6.3) as shown below. The corresponding RA_j values for each (j^{th}) threat is computed using the fuzzy inference system. Then, using the Equation 6.8, the value of $Metric01$ is calculated.

Table 6.4: Computation of $Metric01$ for an example scenario of five (05) identity providers who are vulnerable to different sets of threats.

Identity Provider	Threats	$Metric01$
$IDP01$	[eject, dict, ffb, DDoS 1.0]	0.625
$IDP02$	[perl, dict, ffb, warez, ps]	0.537
$IDP03$	[ps, dict, format, sqlattack, DDoS 1.0]	0.59
$IDP04$	[eject, ps, ffb, DDoS 1.0, DDoS2.0.2]	0.52
$IDP05$	[DDoS1.0, loadmodule, dict, sqlattck, ps, warez]	0.566

6.6.2 $Metric02$ Computation

To compute $Metric02$, a set of attacks with the possible detection and prevention security enforcements (Table 6.5) are considered. It is assumed that the impact (or the consequences) are equal for each of the attacks shown in Table 6.5. Then, possible set of vulnerabilities were extracted from Common Vulnerabilities and Exposures (CVE) repository [CVE 2014]. These are relatively newly discovered vulnerabilities and the possible remedial/preventive solutions to reduce the impact or to mitigate them are use in this analyses. Next, these incidental vulnerabilities are used along with their remedial measures to derive the relative attribute values to compute the $Metric02$ (Table 6.6). As the example scenario a set of identity providers are assumed to have a combination of these enforcements as shown in Table 6.6.

Table 6.5: Security Enforcements for Detection and Prevention of a Set of Known Attacks

No.	Attack	Detection Measures	Prevention Measures	Range of Affiliation Values (minimum - maximum)
A1.	Fraudulent resource consumption attacks [Idziorek et al. 2013]	1.a) Application level log analyzer	1.b) Black listing first time offenders. Impose back-off time-outs to anomalously behaving clients.	(0 - 0.9)
A2.	Hypervisor attacks [Gruschka and Jensen 2010]	2.a) Code integrity measures (e.g. Trustvisor).	2.b.01) Defenses to protect hypervisor code (e.g. HyperGuard), 2.b.02) Input/Output device security (e.g. Bitvisor),2.b.03) functionality shift to user level (e.g. NOVA).	(0 - 0.9)
A3.	XML based denial of service attacks [Chonka et al. 2011]	3.a) Packet level comparing and analyzing against known attack messages.	3.b) Service oriented trace back architecture (message analysis - SOAP message header information [Chonka et al. 2011]).	(0 - 0.9)

A4.	Timing attack [Cleemput et al. 2012][Lombardi and Di Pietro 2011]	4.a) Cache based load measurements	4.b) Compiler based mitigation strategies.	(0 - 0.9)
A5.	Cache-based Side channel attacks [Godfrey and Zulkernine 2013][Zhang et al. 2011]	5.a) Cache usage measurements in selected cache regions.	Blinding techniques such as 5.b.01) cache wiping, 5.b.02) random delay insertions.	(0 - 0.9)
A6.	Load measurements based attacks [Ristenpart et al. 2009][Sundareswaran and Squccia-rini 2013][Sun et al. 2011]	6.a.01) Event-based patterns. 6.a.02) CPU cache usage measurements, 6.a.03) computational load based co-residence detection, 6.a.04) traffic rates measurements to co-resident servers	6.b) Multi-lateral security negotiations based load balancing.	(0 - 0.9)
A7.	Unauthorized data modifications	7.a. Firewall log analyses.	7.b. Robust access control policies.	(0 - 0.9)

- V1 is CVE-2014-0654 Cisco Context Directory Agent Replayed RADIUS Accounting

Message Vulnerability.

- V2 is CVE-2013-6986 Unspecified vulnerability in Oracle Solaris 10 and 11.1 allows local users to affect availability via vectors related to Name Service Cache Daemon (NSCD).
- V3 is CVE-2013-5724 Phpbb3 before 3.0.11-4 for Debian GNU/Linux uses world-writable permissions for cache files, which allows local users to modify the file contents via standard file system write operations. This problem has been fixed in version 3.0.11-4 and expects the users to upgrade earlier versions.
- V4 is CVE-2014-0791 possible patch is available. Integer overflow in the $license_read_scope_list$ function in $libfreerdp/core/license.cin$ FreeRDP through 1.0.2 allows remote RDP servers to cause a denial of service (application crash) or possibly have unspecified other impact via a large ScopeCount value in a Scope List in a Server License Request packet.
- V5 is CVE-2014-0617 Juniper Junos 10.4S before 10.4S15, 10.4R before 10.4R16, 11.4 before 11.4R9, and 12.1R before 12.1R7 on SRX Series service gateways allows remote attackers to cause a denial of service (flowd crash) via a crafted IP packet. Solution is to upgrade to version 10.4S15, 10.4R16, 11.4R9, 12.1R7, 12.1X44, or higher, to address this vulnerability.

Based on the information given in Table 6.6, each identity provider are susceptible to different vulnerabilities in spite of having certain security features installed. Next, using the Equation 6.9, the corresponding $Metric02$ values are calculated (see Table 6.7). Then, the overall trust is computed as the sum of the two corresponding trust values.

Table 6.7: Computation of $Metric02$ for an example scenario of five (05) identity providers who are vulnerable to different sets of threats and vulnerabilities shown Table 6.6.

Identity Provider	k_{dsv}	k_{esv}	$Metric02$

$IDP01$	7	12	0.583
$IDP02$	5	12	0.417
$IDP03$	9	12	0.75
$IDP04$	4	12	0.33
$IDP05$	9	12	0.75

6.6.3 Example

Consider a disaster and crisis management support application, where remote monitoring data from multiple sources (e.g. real-time satellite images, maps) are necessary to access in order to make necessary analyses and critical decisions [Voigt et al. 2007][Roche et al. 2013]. The data is stored in cloud repositories [Klauck et al. 2011][Puthal et al. 2016] and the users are authenticated using the digital identities provided by the identity providers in order to allow access to the data. Consider a scenario where five (05) identity providers are involved in facilitating user authentications.

In order to explain the trust negotiations and identity management, consider a disaster response team leader (User01) needs to access $A2$ application to allocate service requests to restore power at a known location. The authorization requires a set of two (02) identity attributes: $I1$ and $I2$. Chief electrical engineer (User02), requires to access collaborating management application ($A1$) to provision resources to the known location in order to restore the power. The authentication of the chief engineer (or User02) requires two identity attributes $I3$ and $I4$. To compute the $PDCM$, values in Table 6.3 are used. Then, to compute $Metric02$, the attacks and vulnerabilities described in Section 6.6.2 are randomly assigned to each identity provider. Each identity provider is assumed to be susceptible to atleast one vulnerability and one known attack. The security feature sets (see Table 6.6 in Section 6.6.2) are also randomly assigned such that atleast two sets of features are allocated for each identity provider. The value of $Metric01$ is computed for each identity provider as shown in Table 6.4. Next, the trust computation methods

Table 6.6: Relative Stealth ($Metric02$) Estimation Using Fuzzy Equivalence Classes - firewall (F), application log analyses (ALA), antivirus (AV), cache usage measurements (CUM), packet filtering (PF), packet level analyses (PLA), message analysis (MA), event detection at application level (ED-AL), load measurements (LM), automated patch update mechanism (APUM)

Identity Provider	Feature Specifications	Attributes											
		A1	A2	A3	A4	A5	A6	A7	V1	V2	V3	V4	V5
$IDP01$	[F, ALA, AV, APUM]	0.4	0.3	0	0	0	0	0.3	0	0.7	0.7	0.7	0.7
$IDP02$	[F, CUM, AV, MA]	0.3	0	0.3	0	0.3	0.3	0.3	0	0	0	0	0
$IDP03$	[PLA, F, AV, APUM]	0.3	0.3	0	0	0.3	0.3	0.3	0	0.7	0.7	0.7	0.7
$IDP04$	[ED-AL, F, AV]	0.7	0.35	0	0	0	0.35	0.35	0	0	0	0	0
$IDP05$	[LM, F, AV, APUM]	0.3	0.3	0	0.3	0	0.3	0.3	0	0.7	0.7	0.7	0.7
$IDP06$	[F, CUM, PF, AV, PLA]	0.2	0.2	0.2	0	0.4	0	0.2	0	0	0	0	0
$IDP07$	[ED-AL, CUM, F, MA]	0.5	0.3	0.3	0	0.3	0.5	0.3	0	0	0	0	0
$IDP08$	[F, PF, AV, APUM, PLA]	0.2	0.2	0.2	0	0.2	0.2	0.2	0	0.7	0.7	0.7	0.7
$IDP09$	[LM, CUM, F, AV]	0.3	0	0	0.3	0.3	0.5	0.3	0	0	0	0	0
$IDP10$	[LM, F, AV, APUM, MA]	0.2	0.2	0.2	0.2	0	0.2	0.2	0	0.7	0.7	0.7	0.7

described in [Chahal and Singh 2016] and [Ghosh et al. 2015] are compared with the proposed method. To compare with the trust computation described in [Chahal and Singh 2016], since there are no third parties involved, the contribution of the public review trust and auditor trust are considered to be high. This is mainly because the attacks, vulnerabilities and the security features contribute to evidence-based trust (as computed by the $Metric01$ and $Metric02$).

According to the proposed trust based ranking $ID03$, $IDP05$, and $IDP01$ are the most trustworthy. Based on the $PDCM$ value, the identity providers $IDP04$ and $IDP05$ are the most unreliable. The significance of this result for the TCRM application is mainly for User02, it can be assured that the trustworthy $IDP02$ will provide the necessary identities ($I3$ and $I4$) to access the application $A1$ although the cloud service provider initially assumes $IDP02$ to be less reliable. Since the trust computations are based on a pre-defined criteria, despite the initial assumptions, most reliable IDPs can be selected.

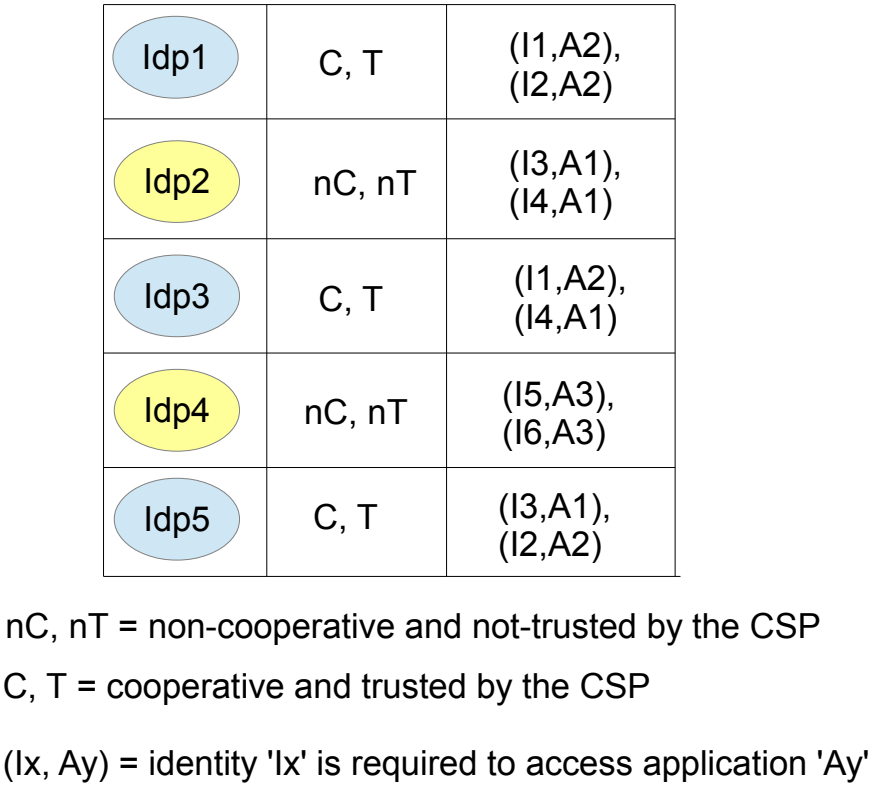


Figure 6.5: Time Critical Disaster Response Management Application - Multiple data access and analysis applications need to be accessed. The necessary digital identities that can be disclosed by each IDP are indicated. At the cloud service provider, the initial guess about the reliability of each IDP is shown.

Next, the identity provider selection using SelCSP [Ghosh et al. 2015] and the indirect trust measurement in [Chahal and Singh 2016] are compared with the proposed model. According the SelCSP [Ghosh et al. 2015], $IDP01$ and $IDP03$ have the lowest risk, thus, more reliable. According to [Chahal and Singh 2016], only $IDP01$ is trustworthy. Although the comparison reveal the identity providers can be selected using the three methods, the main limitation is the dependency of the indirect trust measures when using the methods described in [Ghosh et al. 2015] and [Chahal and Singh 2016]. The proposed trust computation use the evidence-based data to compute the trust associated with the identity providers.

Table 6.8: Comparison of the Selection of IDPs using Different Criteria. Overall trust qualitative scale very high, high, moderate, low and very low get mapped on to [0,2]={2.0,1.5,1.0,0.5,0}

Identity Provider	$Metric01$	$Metric02$	$PDCM$	Overall Trust	SelCSP [Ghosh et al. 2015]	[Chahal and Singh 2016]
$IDP01$	0.583	0.625	3.091×10^5	1.208	2.137	Very high
$IDP02$	0.417	0.537	1.044×10^5	0.954	5.7	Low
$IDP03$	0.75	0.59	1.892×10^5	1.105	1.34	Moderate
$IDP04$	0.333	0.52	459.1×10^5	0.853	6.325	Moderate
$IDP05$	0.75	0.566	62.4×10^5	1.316	4.113	Low

6.7 Comparative Evaluation

In this section, the proposed metrics ($Metric01$, $Metric02$ and $PDCM$) are compared using several existing identity management solutions by using a cloud based trust framework [Arias-Cabarcos et al. 2012b] for federated identity management. This cloud based trust framework compares a federated identity management model based on the pre and post federation phases.

The proposed metrics can be interpreted using cloud based trust framework as follows. $Metric01$ corresponds to integrity and availability aspects of pre-federation phase. $Metric01$ is useful to measure the extent of preserving the integrity aspect attempts to safeguard against improper information modification or destruction and also to ensure availability guarantees against malicious attacks (e.g. denial-of-service). $Metric02$ corresponds to availability. $Metric01$ is useful to measure the extent to ensure availability guarantees against malicious intrusions based on the history of attacks and impacts assessed based on the existing preventive and defensive measures in practiced by a specific identity provider. $PDCM$ corresponds to operational interoperability aspect. $PDCM$ is useful to reveal the policy based constraints between an identity provider and a cloud service provider to carryout a trust negotiation based authentication of a user on behalf

of a SP being serviced by the cloud service provider.

Next, the proposed metrics are compared with the existing cloud based federated identity management solutions: SPICE [Chow et al. 2012], hierarchical cryptography based solution described in [Yan et al. 2009] and ICEMAN [Dreo et al. 2013]. Each of these solutions are interpreted using the TF [Arias-Cabarcos et al. 2012a]. Each existing solution is interpreted based on TF [Arias-Cabarcos et al. 2012a] and compared with the proposed trust based identity provider selection based federated identity management.

In SPICE [Chow et al. 2012], privacy-oriented group signatures with randomization are used to establish authentications with subsequent validations of the attributes used in authentications. This solution corresponds to pre-federation and post-federation authentication and accountability aspects.

In [Yan et al. 2009], federated identity management is used with hierarchical identity based cryptography such that each user and each server will have its own unique identity, and the identity is allocated by the system hierarchically for efficient key distribution and mutual authentications. This solution corresponds to pre-federation authentication and accountability aspects.

ICEMAN [Dreo et al. 2013] uses existing cloud APIs and Federated Identity Management protocols, including the Cloud Security Alliances guidance for Identity & Access Management, Identity Management as as Service (IdMaaS) and the Liberty Identity Federation Framework maintained by the Kantara Initiative. This solution corresponds to both pre-federation and post-federation privacy aspects.

In summary, results (see Table 6.9) reveal that the expressiveness and the suitability of proposed metrics in the proposed trust based identity provider selection method corresponds to the pre-federation phase of federated identity management. Comparison with the existing models based on cloud based trust model [Arias-Cabarcos et al. 2012b] reveals that the proposed metrics are more expressive in all three dimensions of the pre-federation phase while the other solutions are limited to a security and privacy risk dimension.

Table 6.9: Summary of the Analysis of the Expressiveness of the Proposed Three Metrics (Matric01, Metric02 and PDCM) using Existing Cloud based Trust based Framework (TF) [Arias-Cabarcos et al. 2012b] for Cloud based Federated Identity Management

Model	Proposed Metrics	TF [Arias-Cabarcos et al. 2012b]
Proposed Model	Metric01	Pre-federation phase → Security and Privacy Risks → Integrity and Availability aspects.
	Metric02	Pre-federation phase:→ Security and Privacy Risks → Availability aspect.
		Pre-federation phase:→ Knowledge Risks → Direct knowledge aspect.
	PDCM	Pre-federation phase:→ Interoperability Risks → Operational aspect.
SPICE [Chow et al. 2012]	-	Pre-federation phase → Security and Privacy Risks → Authentication and Accountability aspects.
		Post-federation phase → Security and Privacy Risks → Authentication and Accountability aspects.
Hierarchical identity based cryptography for mutual authentications [Yan et al. 2009]	-	Pre-federation phase → Security and Privacy Risks → Authentication and Accountability aspects.
ICEMAN [Dreo et al. 2013]	-	Pre-federation phase → Security and Privacy Risks → Privacy aspect.
		Post-federation phase → Security and Privacy Risks → Privacy aspect.

6.8 Conclusion

The contributions of this chapter provides a set of novel metrics to asses the reliability of an identity provider to participate in the authentication processes of TCRM applications. The metrics were evaluated by mainly using the publicly available data on vulnerabilities and attack scenarios. Based on the analyses using the cloud based trust model [Arias-

Cabarcos et al. 2012b], the proposed trust metrics and the policy based cost metric have demonstrated its apt use compared to other such well known existing cloud based identity management solutions. Based on the findings of this chapter it is evident that the contributions make the cloud based data access in TCRMSs more reliable when there are effective methods to select more reliable identity providers.

6.9 Epilogue

This chapter describes a robust trust based framework for reliable user authentications using cloud based federated identity management. The authenticated user should then be authorized for the data access requests based on the critical situations in TCRMSs.

CHAPTER 7

Context-Aware Content-Sensitive Data Access Control

7.1 Outline of the Chapter

In TCRMSs users access the remote monitoring data from different locations depending on the critical circumstances. These access requests of the remotely logged-in users need to be authorized while ensuring minimum possible permission misuses and potential data disclosure risks. The main contribution of this chapter is a novel location dependent disclosure risk measure, which helps to enforce the situation-dependent access control rules by risk-based validations.

Rest of the chapter is organized as follows. Section 7.2 provides an overview of the research problem and summarizes the contributions. The notations used in this chapter are summarized in Section 7.3. Next, Section 7.4 describes the novel location dependent disclosure risk metric. Subsequently, the Sections 7.6 and 7.5 describe the use of the proposed disclosure risk measure to specify the location-dependent access control rules and break-the-glass rules. Next, Sections 7.7 and 7.8 describe the comparative results. Finally, Section 7.9 concludes this chapter.

7.2 Introduction

In most TCRM applications, during an emergency situation in order to expedite the responses, exemptions are granted to access the remote monitoring data [Crawford and Finn 2015][Xu et al. 2014][Samuel et al. 2014]. It is not an uncommon practice during certain critical emergency situations, to permit otherwise denied data access rights in order to respond faster [Green et al. 2016]. In such situations, it is reasonable to assume that the potential risks of data leakages generated by these violations are lower than the damage caused by a delayed emergency response [Townsend et al. 2006][Scalavino et al. 2010][Carminati et al. 2013]. However, when situation-dependent access requirements are supported by an access control model, the potential disclosure risks and malicious data misuses need to be minimized [Rahimi et al. 2014] [Jaramillo et al. 2013]. It is also important to note that in general, any permission override is inherently associated with risks (including data disclosure risks) [Fugini et al. 2016][Ayed et al. 2014][Dos Santos et al. 2014][Ray and Ray 2014].

During critical situations (e.g. public health emergencies), additional context descriptive information may be useful to enforce situation dependent access rights. Context is defined as any information that can be used to characterize the situation of an entity [Dey 2001]. Examples include time, location, device of access, type of situation (i.e. whether it is an emergency). From the recently reported incidents of remote attacks launched to misuses patient health data [Stevens 2012], it is evident that location can be manipulated to launch confidentiality and privacy breeches. Thus, the location from where a data access is originated becomes an important aspect for a secure repository to consider as an additional contextual information for access control.

The amount of information allowed to access by a user may be susceptible to high disclosure risks due to the location of access over unreliable channels coupled with the associated situation-dependent permission overrides [Freudiger et al. 2011][Liu 2007]. The risk of disclosure of information is the likelihood of violating the privacy of data by a malicious entity within the network or from outside, which can be used to launch attacks to cause undesirable outcomes. For example, in smart grid, the remote monitoring data

were misused to launch malicious attacks by remotely logging into the control system to initiate cascading failures in generators [Wei et al. 2011][Chen et al. 2011]. Although obfuscation techniques are desirable to reduce the disclosure risks, the main disadvantage is a significant loss of information content [Bezzi 2010]. Therefore, in TCRMSs, it is necessary to minimize the potential disclosure risks on the amount of remote monitoring data accessed by the users.

Depending on the context (or the situation), the access control model can alter the permissions of a user depending on the situational requirements. This can be done by enforcing break-the-glass rules [Carminati et al. 2011][Ferreira et al. 2009][Brucker et al. 2010], using permission overrides [Petritsch 2014], enforcing emergency policies [Carminati et al. 2011], implementing adaptive user-role assignment schemes [Ferreira et al. 2009]. A break-the-glass policy can be used in order to violate certain non-permissible authorization assignments or override the existing permissions of a role in a controlled manner. When changing the assigned permissions for each pre-defined role of particular user, it is necessary to ensure that the potential disclosure risks are minimized based on the information content they may be authorized to access during different situations. For example, when there are potential disclosure risks involved in accessing data, it is necessary to enforce the break-the-glass rules to update the permissions of a role depending on the context.

Based on the above discussion, it is necessary to develop new measures which are sufficiently expressive enough to minimize the disclosure risks while enforcing context-dependent access rules.

7.2.1 Limitations of Existing Work

Disclosure risk measures are useful to assess the risks involved in accessing privacy sensitive data. In TCRMSs, depending on the application, different types of data with varying degrees of privacy sensitivity are generated. For example, in remote patient monitoring applications, data related to the health conditions of a patient are recorded and stored in the cloud repositories [Botia et al. 2012][Liang et al. 2012][Thilakanathan et al. 2014]. In the smart grid, various status updates and related electrical measurements are monitored

and stored in cloud repositories to be used by the decision making agents [Cummins 2017].

Based on the discussion provided in Chapter 2, it is evident that all of the existing disclosure risk measures are content dependent and do not express the context associated risks of data. The contributions of this chapter differs from the existing risk based access control models (see Chapter 2) as the location dependencies are used to compute the disclosure risks to enforce the break-the-glass rules in order to satisfy the situational access requirements. The existing location based access control models do not use the location information for enforcing the exemptions (or permission over-rides) depending on the situational requirements [Gupta et al. 2006][Damiani et al. 2007] [Kirkpatrick et al. 2012].

In [Georgakakis et al. 2011], a distance based satisfaction level measure is used to indicate whether a denied request needs to be allowed based on some credible contextual information. This measure evaluates, the extent of the roles of the user (or object), who has submitted (requested) denied access requests which satisfy conditions in the subject specification stated in the access control policy. The proposed model differs from that of [Georgakakis et al. 2011], as location-dependent disclosure risk measure is used as an attribute associated with a role to enforce the situation-dependent break-the-glass rules.

In Ts-RBAC model [Liu et al. 2016], a dedicated transformation policy is introduced to provide user-role assignments depending on the break-the-glass requirements and to subsequently change the permissions accordingly. The proposed model differs from Ts-RBAC due to the use of an attribute to support the permission changes associated with a role rather than to change the user-role assignments depending on the situational requirements.

In BTG-RBAC model [Ferreira et al. 2009], the break-the-glass state is "true" if there is a rule which allows a role to do an operation on an object. Each permission has two states: one permitted under normal conditions and the other for the break-the-glass conditions. Rather than to change the associated permissions of a role, this model use rule based activation of permissions by activating the appropriate role.

The proposed novel solution significantly differs from the above mentioned models when the access request is initiated from a remote location to the network, the authoriza-

tions to access certain privacy sensitive data is decided based on location-dependent data disclosure risks.

7.2.2 Contributions

Contributions of this chapter are summarized as follows:

- *Novel location-dependent disclosure risk computation method* - Novel location dependent disclosure risk estimates are derived at record level and file level. This disclosure risk computation method differs from the existing measures due to its ability to incorporate the location dependent risk. As evidenced by the experimental results and the reliability analysis, the proposed solution is apt for TCRM applications with sensitive data utilizations for situation-specific data utilization requirements.

- *Novel location-dependent disclosure risk constraint based break-the-glass rule enforcement* - Belnap logic is used to enforce the possible break-glass authorizations using the proposed location dependent disclosure risk measure. It is demonstrated how the location dependent risk can be used as a constraint to control the situation-specific authorizations. The expressiveness of the rule enforcements are compared with the existing logic frameworks. Results reveal better expressiveness to achieve break-glass authorizations for confidentiality preserving data access management in TCRMSs.

7.3 Notations

Notation	Description
$LDDR$	location dependent disclosure risk
k_{Np}	population size
k_{ns}	selected sample size ($k_{ns} < k_{Np}$)
$P^x_{y_i}$	probability that an indexed variable y_i is likely to be found in a cell x in the contingency table.

μ_x	probability that a record is unique in a file
π_x	selection probability of elements belonging to a file
$exp()$	exponential function
loc	data access request origin location
Ev_A	event that a user has made a data access request from a known location
Ev'_A	event that a user has not made a data access request from a known location
Ev_{rec}	event that non-trivial record level disclosure risk exists
Ev'_{rec}	complement of Ev_{rec}
Ev_{file}	event that a non-trivial file-level disclosure risk exists
Ev'_{file}	complement of Ev'_{file}
τ_{file}	file level disclosure risk
rep	a particular data representation
$LDDR_{rec}$	location dependent disclosure risk at record level
$LDDR_{file}$	location dependent disclosure risk at file level
Sub	subject
Obj	object
Opr	operation
$role$	role assigned to a subject
$SubId$	subject identifier
$SubContext$	context associated with a subject
CL_{role}	clearance level associated with a role
CL_{obj}	clearance level associated with an object
$ObjId$	object identifier
$ObjContext$	context associated with an object
$Range$	range of an attribute
$Request$	access request
$SecurityRisk(loc)$	security risk associated with the request origin location loc

PL	privacy level
CL_{r_i}	clearance level for a record
CL_{f_i}	clearance level for a file
Thr	pre-defined threshold for the location dependent disclosure risk for a particular situation
$TRUE, FALSE$	binary truth values
$\top$	truth value to express inconsistency as an over-knowledge
$\bot$	truth value to express inconsistency as no-knowledge
L, D, A, V	the events corresponding to location change, LDDR estimate, user authentication and break-glass authorization respectively
ψ_r, ψ_p, ψ_n	the constraints: *responded existence*, *precedence* constraint and *not existence* constraint respectively
e_i	i^{th} event
Tr_i	i^{th} trace
p_{ei}	event probability of the i^{th} event
p_{ti}	trace probability of the i^{th} trace
$p_{e\alpha}$	largest acceptable probability of incorrectly verifying the occurrence of an event
$p_{t\alpha}$	largest acceptable probability of incorrectly verifying the occurrence of an event
k_e	number of experiments conducted

7.4 Location Dependent Disclosure Risk (LDDR) based Data Access

In this section, a novel LDDR based metric and its application to enforce situation-specific access control rules are described. LDDR is estimated to assess the risk associated with

a location change with respect to a known secure location. Depending on the severity of the location based risk involved, the authorization rules based on the context described in terms of the time, location, data content, and the situation are enforced.

7.4.1 Computation of Location Dependent Disclosure Risks (LDDRs)

In this section, the LDDR estimations at the file level and record level [Manrique-Vallier and Reiter 2012] are described. Population size (k_{Np}) is the number of records to which a particular user is given access per access request. This access request may originate from a known secure network or from a remote location.

According to [Manrique-Vallier and Reiter 2012], the record level disclosure risk is probabilistically estimated using the concept of population uniqueness as follows.

$$\mu_x = exp(-k_{Np} P^x_{y_i}(1 - \pi_x)) \tag{7.1}$$

$P^x_{y_i}$ is the probability that an indexed variable y_i (where $y_i \in Y$) is likely to be found in the cell x of a contingency table. It is assumed that the record level representation of the data is generally in the form of tables with finite number of cells. μ_x is the probability that a record is unique in a file when k_{ns} samples of records are selected from a population of k_{Np}. The selection is performed according to Bernoulli sampling with selection probabilities of π_x. In the theory of finite population sampling [Royall 1970], Bernoulli sampling is a process where each element of the population that is sampled is subjected to an independent Bernoulli trial which determines whether the element becomes part of the sample when the elements (e.g. data records, data files) are randomly drawn. In Bernoulli sampling, all the elements of the population have equal probability of being included in the selected sample. Each element of the population is considered separately for the sample.

It is also assumed that the cell count in a contingency table has a Poisson distribution [Chowdhury et al. 1999]. A contingency table refers to a two-dimensional table with finite number of rows and columns [Fienberg 1999][Dobra et al. 2009]. Value in each cell contains private information which needs to be protected. For example, a cell value may contain information of how many times a cancer patient undergoes certain treatments. Consider

$P^x_{y_i}$ as the log-linear estimate on the contingency table. To compute the values of $P^x_{y_i}$, the model described in [Chowdhury et al. 1999], the Poisson probability function is used where the average value varies according to a Gamma distribution. The disclosure limitation literature for contingency table data is highly focus on the risk-utility trade-off [Dobra et al. 2009]. The risk is measured in terms of information contained in marginal tables for small cell counts, by computing the bounds for cell entries, or by counting of possible table realizations [Dobra et al. 2009][Fienberg and Slavkovic 2005]. However, when there are contextual dependencies additional factors should be considered to compute the associated disclosure risks.

Next, Bayes theorem is used to extend the record level disclosure risk with location-dependent risk. Bayes theorem is useful to compute the conditional probabilities of different events. Suppose Ev_A is the event that the user has made the data access request from a particular known location, then Ev'_A is the event that it is not from the known location. The event Ev_{rec} represents the existence of a non-trivial record level disclosure risk of a record (i.e. μ_x) when responding to a request initiated from the known location. Then, the location dependent record level disclosure of risk ($LDDR_{rec}$) can be computed as follows (Equation 7.2),

$$LDDR_{rec} = \frac{P(Ev_A|Ev_{rec}).\mu_x}{P(Ev_A|Ev_{rec}).\mu_x + P(Ev'_{rec})P(Ev_A|Ev'_{rec})} \tag{7.2}$$

Similarly, the file level risk τ_{file} [Manrique-Vallier and Reiter 2012] can also be estimated as follows. The main assumption is that the number of record level sample unique records is also population uniques at the file level. The sample uniques are those records with highest risks which are the combinations of values of the key variables that are unique in the data sample. Generally, the sample unique records are identified based on a probability model (e.g. Poisson, log-linear) [Bethlehem et al. 1990] which generates the frequencies of the values of the key variables. Then, for a given data representation rep, the associated file level risk is equal to the sum of record level risks (for each record x).

$$\tau_{file,x} = \sum_{\{x:rep_x\}} \mu_x \tag{7.3}$$

It is important to note that the file level and record level disclosure risk measures provide different disclosure risk interpretations for a population size k_{Np}. The file level disclosure risk averages the risk across the whole data sample. The record level measure helps to identify those parts of the sample where disclosure risk is high. Next, to compute the location dependent file level risks, the Bayes theorem is used. Consider Ev_{file} to be the event that a non-trivial file level disclosure risk (i.e. τ_{file}) exist. Then, the location dependent file level disclosure of risk ($LDDR_{file}$) can be computed as follows (Equation 7.4),

$$LDDR_{file} = \frac{P(Ev_A|Ev_{file}).\tau_{file}}{P(Ev_A|Ev_{file}).\tau_{file} + P(Ev'_{file})P(Ev_A|Ev'_{file})} \tag{7.4}$$

7.5 Use of LDDR Measures for Access Control

In this section, the use of LDDR for access control is described using the subject specification based on RBAC-A [Kuhn et al. 2010]. RBAC-A is a combination of role based access control and attribute based access control. The definition of a role, object, permission are as defined in the seminal paper of [Kuhn et al. 2010]. As mentioned before, RBAC-A [Kuhn et al. 2010] is used to define the subjects and objects with the associated attributes ($SATT$ and $OATT$ respectively). Continuing from [Kuhn et al. 2010], the role centric addition elaborated in [Jin et al. 2012]. An attribute is defined as a function which takes certain inputs and returns values for the defined properties of that input. Each subject and object is associated with a finite set of attributes. The advantage of this approach is the ability to retain the maximum set of permissions for a particular role.

The upper bound of the amount of confidential information resources that are allowed to access is determined based on the *clearance level* assigned to the role and *privacy levels* associated with the data records (or files). Assigning a content dependent *privacy level* is useful when different types of data are generated in a TCRMS. For example, in a distributed power generation remote monitoring system with cloud based data storage and access management (e.g. Netbiter [Netbiter 2017], Cummins solutions [Cummins 2017]), there are various data logs accessed to make the necessary time critical decisions. Power

generation remote monitoring system generates different set of data, such as annunciator, alternator and engine data, transfer switch data, source, load and switch connection status etc [Cummins 2017]. Different data are useful for remote operations and maintenance functions. Therefore, the necessity to manage who gets to access which type of data with minimum disclosure risks.

Each user (or a subject) is assigned with roles. Roles take values equivalent to the job title or the designation based on the organizational hierarchy [Kuhn et al. 2010]. Examples of include manager, engineer, accountant etc. For a subject, there is a subject identifier *SubId* which takes the value of the name of the user. Additional attributes are defined to express the context ($SubContext = \{SCloc, SCtime, SCsit\}$) including location, time, situation respectively. In addition to the *SubContext* and the *SubId*, a *clearance level* (CL_{role}) is defined as the maximum tolerable data access risk associated with the *role* of the *Sub*.

Objects are the files or the data records. Each object has an identifier (*ObjId*) and associated context attributes for location, time and situation as, ($ObjContext = \{OCloc, OCtime, OCsit\}$). Similar to a role, object clearance level CL_{obj} is defined. The CL_{obj} is estimated using the *privacy levels* (PL) of the objects. The PL values are assigned based on the contextual information and content associated using expert knowledge. For a particular record r_i, $CL_{r_i} = PL_i$. For a particular file f_i, which is a collection of n records, $CL_{f_i} = \frac{\sum_{i=1}^{n} PL_i}{n}$. The associated attributes can be categorized based on the number of possible values they can take. Each attribute can take a single value (i.e. atomic) or a set of values known as the *Range* (Table 7.2).

In general, a data access request tuple $Request =< Sub, Obj, Opr, role >$ gets interpreted as follows [Kuhn et al. 2010]. The access control model verify whether the subject *Sub* under the permissible *role* based on the role assignment rules. Then, verifies whether this *role* can access the requested object *Obj* based on role object assignment rules. Subsequently verifies, whether the *role* is allowed to do the intended operation *Opr* on *Obj* based on role permission assignment rules.

In this chapter, it is assumed that when a user initiate a request, the access control model interprets it as:

Table 7.2: Different Types of $SATT$s and $OATT$s.

Attribute	Attribute Type
$SubID$	set
$SubContext_{loc}$	set
$SubContext_{time}$	set
$SubContext_{sit}$	set
CL_{sub}	atomic
$ObjID$	set
$ObjContext_{loc}$	set
$ObjContext_{time}$	set
$ObjContext_{sit}$	set
CL_{obj}	atomic

$Request =< Sub, loc, Obj, Opr, role >$.

The additional context information of the location of origin of the access request is included. Also, it is assumed that there exists known risk ($SecurityRisk(loc)$) associated with the request initiating location (loc) for a user to have remote access to the intended network. Also, the $role$ gains access to the Obj if and only if $CL_{role} \geq CL_{obj}$.

7.5.1 Example

Consider a power generation remote monitoring system with cloud based data storage and access management (e.g. Netbiter [Netbiter 2017], Cummins solutions [Cummins 2017]). The remote monitoring data can be accessed by the authorized users from anywhere through smart computing devices. For such a remote monitoring system, use of the above formulated attribute centric model to access the collected data is described in the following scenario.

DecisionAgent and *Machine* are two roles in a power plant. These subjects are allowed to remotely read the *error-log* and *status-file* for remote operations and maintenance at any time provided the subject authenticates. The request will only be approved if the access is from the network locations $nl1$, $nl2$ or any other location loc if the associated $SecurityRisk(loc) < SecurityRisk(nl1)$ and $SecurityRisk(loc) < SecurityRisk(nl2)$. According to RBAC-A [Jin et al. 2012], the attribute types, ranges, and the permission filtering policy which contains the constraints (described as filtering functions) should be described. For the above scenario, the basic sets (Sub, Obj) associated with different

types of attributes ($sttType$), possible values for the attributes (or the range $Range$) functions ($FMachine$, $FLocRiskAuthorized$, and $FAuthorized$) and the filtering policy ($TargetFilter$) are described below.

$Sub = \{decisionAgentof, uloc, stype\}$

$Obj = \{type, recordof, oloc, optype\}$

$attType(decisionAgentof) = set$

$attType(sptype) = attType(otype) = set$

$attType(oloc) = attType(uloc) = set$

$attType(type) = attType(recordof) = atomic$

$Range(type) = \{statusfile, errorlog, alarmindicatorfile\}$

$Range(decisionAgentof) = Machine$

$Machine$s are those which are remotely monitored at the plant, Machine $\subseteq$ U

$Range(recordof) = U$

$Range(uloc) = Range(oloc) = \{nl1, nl2, nl3, nl4\}$

$Range(optype) = Range(sptype) = \{low, medium, high\}$

$FILTER = \{FMachine, FAuthorized, FLocRiskAuthorized\}$

$FMachine(se : SESSION, o : Obj, read)$

{

$recordof(o) \in decisionAgentof(sessionowner(se)) \bigotimes (sptype(decisionAgentof(session(se))) \geq optype(o))$

}

$FAuthorized(se : SESSION, o : Obj, read : Opr)$

{

$(\forall nl1 \in oloc(o). \forall nl2 \in oloc(o) \in uloc(sessionowner(se).nl1 = nl2)) \bigwedge$

$(device(sessionowner(se)) \in setofapprovednetworkdevices) \bigwedge$

$(time(session(se))$ **if**

$acceptedObl(decisionAgentof(sessionowner(se)), time(sessionowner(se), login, T_{window}))$

}

$FLocRiskAuthorized(se : SESSIONS, o : Obj, read : Opr)$

{

$(\forall L_k \in sloc(o).\forall L_k \in oloc(o) \in (SecurityRisk(L_k) < SecurityRisk(nl1)) \bigvee (SecurityRisk(L_k) < SecurityRisk(nl2))) \bigwedge$

$(device(sessionowner(se)) \in setofapprovednetworkdevices) \bigwedge$

$(time(session(se))$ **if**

$acceptedObl(decisionAgentof(sessionowner(se)), time(sessionowner(se), login, T_{window}))$

}

$TargetFilter(se : SESSION, o : Obj, read : Opr)$

{

$filter\{\}$;

$casetype(o) = statusfile : filter = filter \bigcup (FMachine \bigcup FAuthorize \bigcup FLocRiskAuthorize)$;

$casetype(o) = errorlog : filter = filter \bigcup (FMachine \bigcup FLocRiskAuthorize)$;

}

Based on the above example, it is clear that the enforcement of the access control rules with location dependent risks provides more flexibility to control the situation specific data access requests in TCRMSs.

7.6 Use of LDDR to Enforce Break-the-Glass Authorizations

Break-glass rules allow users to grant permissions by overriding access control decisions based on critical situation specific requirements. The most common method is to use temporary user accounts associated with powerful access rights. This approach is not secure as access control is enforced in an ad-hoc manner with little scope to verify the override decisions. Therefore, it is vital to integrate break-the-glass rules to realize more flexible access management. In the recent past, break-the-glass solutions are integrated by using obligatory support measures and explicit confirmations of overrides [Brucker and Petritsch

2009][Marinovic et al. 2014]. Situation dependent access requirements demand break-the-glass enforcements without compromising security in terms of misuses of sensitive data. In this chapter, the LDDR is used a decision support measure for reliable enforcement of situation-specific access requests.

Since LDDR is both a context and content based risk measure, knowledge based logic representation is suitable to express the formation of rules. Belanp logic is selected as it is a knowledge based logic representation [Belnap Jr 1977]. Belnap logic is composed of four truth values. These four truth values can be described based on the difference in the amount of knowledge each value exhibits. With sufficient knowledge there are two truth values $TRUE$ and $FALSE$. When there is a conflict, inconsistency expressed as an over-knowledge the truth value is expressed as $\top$. When there is no knowledge the truth value is denoted by $\bot$ [Belnap Jr 1977]. Rumpole's enforcement model [Brucker and Petritsch 2009][Marinovic et al. 2014], which is based on Belnap logic use three types of rules, applicability rules, evidential rules and positive break-the-glass rules [Marinovic et al. 2014]. These three types of rules are used to compose the situation-specific break-the-glass rules by using the LDDR to enforce break-the-glass access control requirements. Evidential rules are used to define how LDDR is used to specify the extent of feasibility to override request based on a contextual description.

Positive break-the-glass rules define the obligatory re-authentications. In order to verify the positive break-the-glass rule enforcement, the formulation given in [Brucker and Petritsch 2009] is used. Verification of enforcing a positive break-the-glass rule is important to reduce the risks of disclosure in accessing sensitive data. The applicability rules are used to include the conditional requirements. In order to enforce the break-the-glass applicability rules with LDDR estimates, the **if** which is known as the applicability operator [Brucker and Petritsch 2009] is used. Consider the scenario of allowing a *decisionAgent* to read any target log file at anytime from a location *loc*, provided that LDDR is lower than a threshold (Requirement01). Following *applicability rule* defines this requirement.

$$competent(Sub, Read, Obj) \Leftarrow role(Sub, decisionAgent)\,\textbf{if} \quad clearance(Obj, \text{LDDR}, Thr) \tag{7.5}$$

The notational presentations are Sub - subject, Act - action (where Act = Read), $Obj = file, record$ - target object (a record or a file), and Thr - pre-defined threshold for the location dependent disclosure risk for a particular situation. There are two applicability conditions for this rule: i) for the role to be a $Nurse$ and ii) the LDDR to be maintained at a maximum Thr.

In order to ensure reliability, the positive break-the-glass rules (i.e. a type of evidential rules [Marinovic et al. 2014]) are defined to grant an override when a possible set of obligations are specified. For example, a *decisionAgent* (where $Sub = decisionAgent$) is permitted to write on to a *MaintenanceUpdate* file when that user is already allowed to read it and has agreed to provide the reason for it (Requirement02). This can be enforced by the following *enforcement rule*.

$$permit(Sub, file, append) \Leftarrow competent(Sub, file, Read)\,\textbf{if} \quad agreedObl(Sub, log, giveReason) \tag{7.6}$$

Furthermore, in order to ensure a reliable enforcement of the above positive break-the-glass rule, a break-the-glass resolutions query is also enforced to validate the rule content.

$$\Omega(permit(Sub, file, append) \geq_t \top) \wedge (deny(Sub, file, append) \leq_t \bot) \sqsupset_t (deny(Sub, file, append <_t t) \wedge agreedObl(Sub, reAuth, give)) \tag{7.7}$$

where Ω is a break-the-glass resolution query where the permission override is granted based on the positive break-the-glass rule if and only if the obligatory re-authentication (demoted as $reAuth$) is successful. This enforcement ensures appropriate conditional constraint enforcement of a break-the-glass rule for accessing a data file.

7.7 Comparative Analysis of the Expressiveness of Break-glass Authorizations

In this section, the expressiveness of the LDDR based rules to enforce situation-specific requirements using Rumpole break-glass model [Brucker and Petritsch 2009][Marinovic et al. 2014] is compared with several well-established logic frameworks, described in [Bertino et al. 1999] and [Jajodia et al. 1997]. Rumpole is a Belanp logic based break-glass model. The enforcement of the break-glass rules using LDDR measure for specific requirements.

Comparison of the semantics of the three logic frameworks are shown in Tables 7.3 and 7.4. Discussions on the results obtained with the rule specification in each logic framework are presented in subsequent sections.

7.7.1 Using Authorization Specification Language (ASL)

The Authorization Specification Language (ASL) described in [Jajodia et al. 1997], use six types of rules and semantics specified to enforce the example authorization requirements described in Section 7.6. With ASL, the break-glass authorizations using LDDR is expressed as a closed policy. The reason is the inability to confirm the possible LDDR values corresponding to a known set of secure locations as opposed to explicitly specifying all possible insecure locations (as required in an open policy).

- Requirement 01- A user with an authorized role of a *decisionAgent* is able to *Read* a *statuslog* provided that LDDR is maintained lower than a threshold.

$$grant(o, u, r, +Read)$$
$$\leftarrow dercando(o, s, +Read)\&\ do(o, s,\ Read)\&R \subset decisionAgent\&r \in R$$
$$\leftarrow done(o', u, R, +Read, 1)\&typeof(o', l)$$

- Requirement 02 - A subject ($r = decisionAgent$ and $u = user$) is permitted to write on to a $o = MaintenanceUodate$ file when it is already allowed to read it and has agreed to provide the reason for performing a *write* operation.

Table 7.3: Comparison of the Semantic Support of Logic Frameworks for Expressing Break-Glass Authorization Rules Using LDDR

Semantic Support for Expressiveness			
Properties Logic Framework	Rumpole model [Brucker and Petritsch 2009][Marinovic et al. 2014]	LFM01 [Jajodia et al. 1997]	LFM02 [Bertino et al. 1999]
Rule Types	evidential rules, break-glass rules, grant policies	resolution rule, access control rule, authentication rule, derivation rule, done rule, integrity rule	authorization rules, support rules
Predicates	subject, target, action, accepted, context, grant, request-obligations, deny	cando, do, dercando, grant, done, active, dirin, in, typeof, error	auth, action, object, user defined predicates, variable symbols (self)
Evaluation Decisions	grant, deny, request-obligations	grant, deny	grant, deny
Additional Features	query operator, priority override operator, majority rule for overrides	General override approaches: sub-subject, path and no overrides. General conflict resolution approaches: denial-take precedence, permission take precedence, nothing takes precedence.	Users, groups and their hierarchies exist. General override approaches: sub-subject, path and no overrides. General conflict resolution approaches: denial-take precedence, permission take precedence, nothing takes precedence.
Break-glass rules and related policies	positive rules, negative rules, composite rules	Not supported.	Not supported.

$$grant(o, u, r, +Write)$$

$$\leftarrow active(u, r) \& r \in R \& R \subseteq decisionAgent \& do(o, +Read)$$

$$\leftarrow done(o, u, R, +Oblig)$$

– Additional resolution rule is used to distinguish between distinct LDDR values corresponding to two locations $l1$ and $l2$.

Table 7.4: Comparison of the Logic Frameworks for Break-Glass Authorization Rule Enforceability Using LDDR

Semantic Support for Enforceability			
Properties Logic Framework	Rumpole model [Brucker and Petritsch 2009][Marinovic et al. 2014]	LFM01 [Jajodia et al. 1997]	LFM02 [Bertino et al. 1999]
Ability to express Requirement01	Rules are well defined to completely express this requirement (see Expression 7.6)	Sufficient number of rule types to express the specific predicates. Limited number of predicates with fixed arity and attribute types. No flexibility for user defined predicates to associate additional attributes. (see Expression 7.8)	Limited number of rules and predicates (see Expression 7.8).
Ability to express Requirement02	Rules are well defined to completely express this requirement (see Expression 7.7). In addition to completely express this requirement using a resolution query (see Expression 7.8).	Limited number of rules and predicates. No flexibility for user defined predicates to associate additional attributes. (see Expression 7.8 and 7.8)	Limited number of rules and predicates. Flexible to define new predicates with fixed arity (see Expression 7.8).

$$error \leftarrow done(o, u, r, +Read, t)\&$$
$$done(o, u, r, +Read, t')\&$$
$$typeof(o, l1)\&typeof(o, l2)$$

Compared to the LDDR based break-glass rules formulated using Rumpole break-glass model in Section 7.6, the enforcement and applicability rules for Requirement01 cannot be completely expressed as the $type(o', l)$ is limited to a single LDDR value. Since the predicates *do*, *done*, *decando*, and *cando* cannot be expressed for other object types, the obligatory requirements cannot be verified and validated. Since there is limited scope of

using a resolution rule in ASL, the intended resolution query described using the Rumpole model [Marinovic et al. 2014] can only be stated in response to the Requirement02. In order to have the required obligatory response validation expressed using Rumpole model [Marinovic et al. 2014], it is assumed that there is a specific task *Oblig* which represent the obligatory completion of a validation. Additional resolution rule in terms of an error is specified for two distinct LDDR values on the same object and the same role.

7.7.2 Using Authorization Logic Framework

Next, the expressiveness of the above two requirements using the authorization logic framework [Bertino et al. 1999] is compared.

With this logic framework, the break-glass authorizations using LDDR is most feasible to express as a closed policy. The reason is the inability to confirm the possible LDDR values corresponding to a known set of secure locations by using the user defined predicate symbols.

- Requirement 01- A user with an authorized role of a Nurse is able to Read an electronic health record provided that LDDR is maintained at a threshold.

$$(o, s) : \{r1 : auth(read, g) \leftarrow val(type(lddr, th)),$$
$$r2 : val(lddr, th) \leftarrow (self, X) \& auth(read, Y) \& X \neq s\}$$

- Requirement 02 - A subject is permitted to write on to an electronic health record file when it is competent to read it and has agreed to provide the reason for it

$$(o, s) : \{r1 : auth(write, g) \leftarrow val(auth(read, g))\}$$

When specifying the domain for Requirement01, for object o and subject s is authorized to perform the action 'write' on o if there is no authorization for anybody else to write on o. The user-defined predicate *val* is used to validate the value of LDDR and

the competence of the associated subject to perform the action 'read' on o. One of the limitations of using this logic framework is the inability to specify the existence of the a specific active role 'Nurse'. However, it is not feasible to specify a resolution query developed using the Rumpole model [Marinovic et al. 2014] due to the limitations of the logic framework. In order to compare the performances of break-glass authorization rule specifications using the above mentioned logic frameworks, properties described in [Tonti et al. 2003] have been used. Expressiveness is defined as the ability to handle the wide range of policy requirements. Simplicity is defined as the ease of the policy definition tasks based on the semantics specified for a specific framework. Enforceability is defined as the ability to ensure a mapping of authorization requirements into implementable policies.

Based on the rule specifications and the comparative analysis, it is evident that the expressiveness of the authorization rule enforcements using the Rumpole model [Marinovic et al. 2014] is higher compared to the other existing logic frameworks (see Tables 7.3 and 7.4). Based on the results, it is evident that the Rumpole model [Marinovic et al. 2014] provides better rule specification semantic support than the existing logic frameworks.

7.8 Logical Constraints based Verification of Situation Specific Authorization using LDDR

Next, the application of LDDR as a reliable constraint for access control is demonstrated. In a reliable system, a set of events are allowed to occur under certain constraints [Rausand and Høyland 2004]. Based on a set of pre-defined constraints, a trace of events can be declared as valid if the constraints are not violated. In order to perform such an analysis for finite set of possible event traces, a declarative process language called Declare language [Pesic et al. 2007] is used along with runtime verification - finite linear temporal logic (RV-FLTL) [Bauer et al. 2010]. RV-FLTL is a variant for finite traces based on LTL. The Declarative language is used to state the constraints of the events in order to develop a feasible constraint model. To perform state based analysis of the constraints, deterministic finite automata are developed using the semantics of RV-LTL for each constraint using the translation as described in [Giannakopoulou and Havelund 2001]. The constraint model

is shown in Figure 7.1.

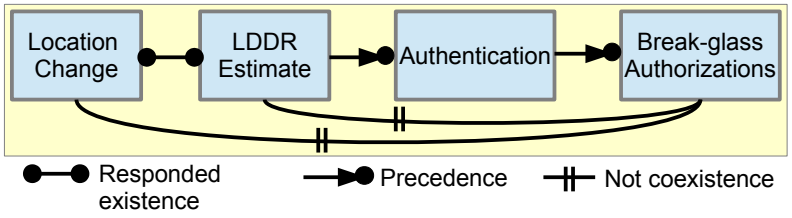


Figure 7.1: Constraint model for the Proposed LDDR Framework

Four main events of the situation specific authorization are defined as: (i) location change (L), (ii) situation-dependent risk variation computed using LDDR estimate (D), (iii) user authentication (A) and (iv) break-the-glass authorization (V). The upper-case letter is used to denote each event. For these four events, the constraint model is developed as shown in Figure 7.1. These events are allowed to take place if certain conditions are satisfied. These conditions are described as constraints. Based on the semantics described in [Pesic et al. 2007], the three constraints are constructed as follows. ψ_r is the *responded existence* constraint, ψ_p refers to the *precedence* constraint and ψ_n corresponds to *not existence* constraint. For each constraint the deterministic finite automaton is computed (see Figure 7.2). The $S0$ indicates the initial state. An accepting state is indicated using double lines. The gray background corresponds to permanent states.

Local automata describes each constraint but does not monitor all the constraints collectively. Based on the local automata for all three constraints, the global automaton is computed as shown in Figure 7.3. The global automaton the product of all three local automata are used. A state in the global automata represents the states in constraint ψ_n, ψ_p and ψ_r respectively.

In order to evaluate the traces mentioned above, probabilistic approaches are recommended [Younes et al. 2006][Sammapun et al. 2005][Filieri et al. 2011]. An event is defined as an instance of an action or a change in a condition [Talcott 2008][Rajkumar et al. 2010]. Depending on the TCRM application, the possible set of events may vary.

Consider for each event, there is an associated probability which is defined as the event probability (p_{ei}). To compute p_{ei}, consider there are k_e number of experiments

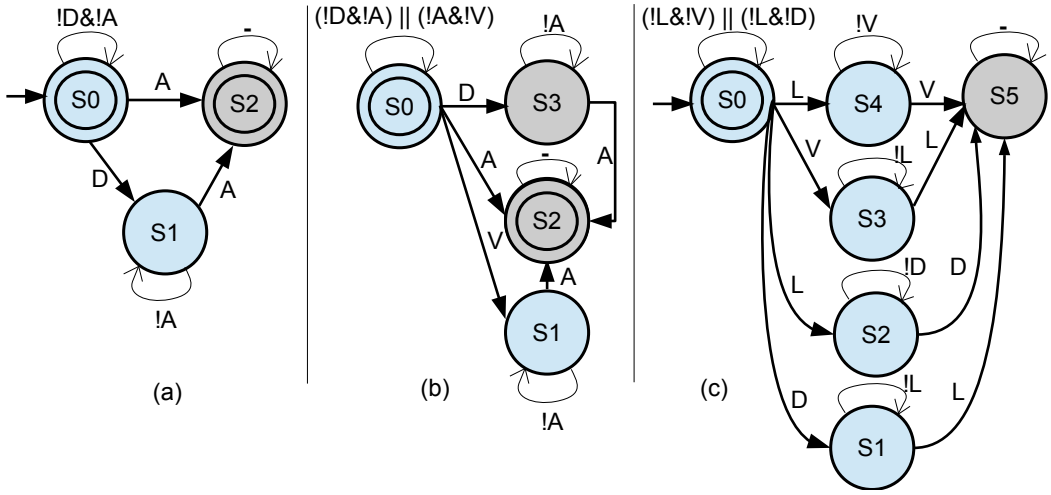


Figure 7.2: Deterministic Finite Automaton Interpretation for Each Constraint: (a) ψ_r - *responded existence* constraint, (b) ψ_p - *precedence* constraint and (c) ψ_n - *not existence* constraint. The corresponding states inferred from the constraint model (see Figure 7.2) are shown here.

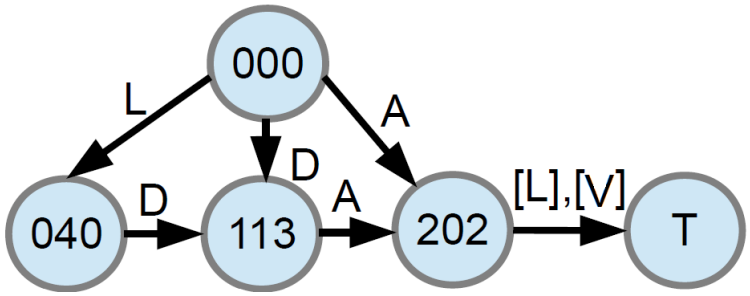


Figure 7.3: Global Automaton for the Three Constraints.

conducted. If the particular event e_i occurs (i.e. $e_i = 1$), then, such occurrences are counted. If that event does not occur it is recorded as $e_i = 0$. Then, $p_{ei} = \frac{\sum e_i}{k_e}$ [Sammapun et al. 2005]. Once the event probabilities are calculated, the corresponding z-scores are calculated [Sammapun et al. 2005] by using the formula $\frac{p_{ei} - p_{e\alpha}}{\sqrt{\frac{p_{ei}(1-p_{ei})}{k_e}}}$. Depending on the constraints applied to $p_{v\alpha}$, the z-score values vary. The authors in [Sammapun et al. 2005] propose to use two error bounds, the largest acceptable probability of incorrectly verifying a true property (or the occurrence of an event) and the largest acceptable probability of incorrectly verifying a false property. Property herein describes the verifiable information (or identification) that a particular event has occurred. For example, the event of a successful log-on is indicated in the access control logs. The occurrence of an

event is accepted if and only if the z-score is less than the largest acceptable probability of incorrectly verifying a true property (or the occurrence of an event) and if $p_{ei} < p_{e\alpha}$.

A trace is defined as a set of consecutive events over a period of time. The minimal length of a trace is two events. Similar to the above formulation, p_{ti} is defined as the trace probability. A trace is considered to be acceptable only if it satisfies the order of the events permitted by the constraint model (shown in Figure 7.3). Such permissible trace occurrences are recorded ($\sum Tr_i$) for each permissible trace over k_e number of experiments. The ratio between $\sum Tr_i$ and k_e.

Example: Consider an example scenario of a remote patient monitoring application with 10 users (03 doctors, 02 nurses, 02 clerks, and 03 patients.). These users may require to access the health data of the patients. Due to the nature of this TCRM, in order to compute whether an event occurred (or not), the following assumptions and the verifiable actions are considered.

1. *Assumption01:* The break-glass accounts are created using verifiable naming convention by authorized high management users.

2. *Assumption02:* There are sufficient detection controls to verify the logged-on (or used) break-glass user accounts.

3. *Assumption03:* Authentication of the users are performed by the trust negotiations or using fixed credentials.

4. *Assumption04:* Remote log-on actions are verifiable based on the location verification alerts.

5. *Assumption05:* Log-on request of the user contains verifiable situation specific information to compute the associates risk when compared to a pre-defined log-on type (e.g. log-on to the network from a fixed network address) for a particular user account.

Next, based on the above assumptions for each event L, D, V and A, following verifiable actions were considered for the analysis (see Table 7.5). Then, for each event, the following failure conditions are considered.

Table 7.5: Verifiable Actions for Each Event L, D, V and A.

Event	Verifiable Actions
L	Location verification alerts
D	Situation specific risk alerts
V	Break-the-glass accounts log-on alerts
A	User account log-on alerts

Table 7.6: Failure Conditions for Each Event L, D, V and A.

Event	Failure Conditions
L	Location verification failure: incorrect location information, responded outside the allowed time
D	Situation verification failure: incorrect information to validate the situation, responded outside the allowed time
V	Risk assessment failure: responded outside the allowed time
A	Authentication failure: incorrect credentials, responded outside the allowed time, attempts to use already disabled or expired accounts

A simulation was run over 1000 times using the set of 10 users, where each user is given a username (two digits) and a password (randomly chosen four digit number). Each user request contain the information about the user account, situation specific content, and the location. The user can authenticate using these pre-defined log-on credentials or can opt to use a trust negotiation process. In addition to these user accounts, break-glass accounts are also pre-defined using the suffix "BRxx", where 'xx' are two digits. Then, depending on the user inputs, the location is verified for each user account. The location identities are assumed to be known to the users. If it is an unknown location, it is assumed to have failed the location validation. Periodically, the location is validated. For this experiment 10s was selected as the location validation period. Based on the empirical results published in [Freudiger et al. 2011], it is considered that the location risk may take a value in the range of 0.2 to 0.8, where 0.2 indicates a lower risk than when it is 0.8. According to the published results in [El Emam et al. 2011], it is considered that the average record level disclosure risk if 0.338 for the health data. For each simulation run, the

selected location risk and the average record level risks, the corresponding LDDR values are computed as per the Equation 7.2. There are pre-defined situation specific information and corresponding risks. Based on the user inputs, the associated risks are calculated. When the break-glass user accounts are logged-on, separate location and situation specific content validations are performed and the event are recorded onto a text file. Possible events are shown in Tables and 7.6. Each event (including both failure and success events) is given a number $Evxx$, where xx ranges from 00 to 12.

Table 7.7: Computation of Event Probabilities for $k_e = 1000$.

Event	$\sum e_i$	p_{ei}	z-score		
			$p_{e\alpha} = 0.1$	$p_{e\alpha} = 0.3$	$p_{e\alpha} = 0.7$
L	236	0.23	16.53	15.02	12.02
D	149	0.15	4.43	-4.43	48.715
A	562	0.56	9.38	5.31	2.85
V	53	0.05	8.33	41.65	108.33

Table 7.8: Computation of Trace Probabilities based on the Constraint Model in Figure 7.3 and $k_e = 100$.

Trace	$\sum Tr_i$	p_{ti}	z-score		
			$p_{t\alpha} = 0.1$	$p_{t\alpha} = 0.3$	$p_{t\alpha} = 0.7$
LD	53	0.53	8.61	4.69	-3.469
DA	47	0.47	7.41	3.46	-4.693
AL	21	0.21	2.7	- 2.211	-12.039
AV	34	0.34	5.066	0.851	-7.659
LDA	48	0.48	7.606	11.83	-4.489
DAL	35	0.35	5.241	1.063	-7.44
DAV	45	0.45	7.03	3.061	5.102
LDAV	30	0.30	8.61	0	8.728
Other	13	0.13	0.892	5.059	16.97

The events and the traces summarized in Tables 7.7 and 7.8 reveal that for a lower values of $p_{e\alpha}$ and $p_{t\alpha}$, the z-score values are larger. The trace and event analyses component of an operational support system of a remote monitoring system essentially need to allow only if 'A' has occurred as the first event. On the other hand, to prevent progressing an attack, the operational support system can declare a vulnerability if the first and the second events that are occurred are 'L' and 'A' respectively. For other traces which do not comply with the permissible traces according to the constraint model shown in

Figure 7.8 occurred during the simulations. These traces were indicated as not accepted traces. Based on the results, by using a constraint model and pre-defined possible events, it is possible to identify the permissible traces and events and to quantify the occurrence probabilities and comparatively asses their significance. The limitation of this analyses includes the number of traces and events involved and the specific scenario.

7.9 Conclusion

In this chapter, the main contribution is a novel location dependent disclosure risk computation method to enforce situation-dependent authorizations rule specifications due to remote data access in TCRMSs. Usefulness of the proposed disclosure risk computations in enforcing situation specific break-glass authorization policies were demonstrated using Rumpole: a Belnap logic based break-glass model [Marinovic et al. 2014]. When compared with the other well known logic frameworks, the expressiveness of the break-glass rules using the semantics of the Rumpole model [Marinovic et al. 2014] and the proposed location dependent disclosure risk measure provided greater flexibility. The results also reveal that the proposed location dependent disclosure risk computation method is a reliable constraint enforcement mechanism.

CHAPTER 8

Conclusion

This research was set to explore the two significant dependability factors: reliability and security of sensed data transmission and access in time critical remote monitoring applications. The research questions address the limitations of existing methods and propose novel solutions which resulted the following contributions.

- A multi-attribute trust metric as a decision support tool for accurate and reliable spectrum hole detection while avoiding malicious spectrum sensing data falsification attackers from participating in cooperative spectrum sensing (Chapter 03).
- A reliable delay-bounded persistent data transmissions for the re-entrant SUs when there are multiple interruptions on sensed spectrum channels (Chapter 04).
- Energy-aware PUF-based encryption key size selection to minimize pattern reproducibility to ensure secure and reliable sensed data transmission (Chapter 05).
- Trust based cooperativeness assessment for cloud-based digital identity management for reliable user authentications (Chapter 06).
- Context-aware disclosure risk based situation-specific authorization enforcement method for reliable data access (Chapter 07).

In summary, the Chapters 3, 4 and 5 describe solutions for reliable and secure data transmission over unreliable wireless channels. Chapters 6 and 7 describe the solutions in

terms of robust user authentications with context-aware situation specific authorizations for reliable and secure data access.

Future Work

As future work, the usefulness of multi-attribute trust metric described in Chapter 03 is extended as a decision supporting measure to determine the priority among the secondary users for channel allocation in TCRMSs. As an extension of the contributions in Chapter 04, it is anticipated to explore the impact of spectrum pricing for multiple re-allocations for the interrupted secondary users in TCRMSs with different traffic classes. As future work, the contributions of Chapter 05 is extended by incorporating the stochastic deterioration models to model the life-time of the sensor nodes to further investigate the dependabilities on the encryption key size for secure transmissions in TCRMSs. To extend the contributions of Chapters 6 and 7, by incorporating the device dependencies and connectivity constraints to account for the robust user authentications to enforce adaptive context-aware situation-specific authorizations in TCRMSs with high variety and veracity data.

Bibliography

J. H. Abawajy and M. M. Hassan. Federated internet of things and cloud computing pervasive patient health monitoring system. *IEEE Communications Magazine*, 55(1): 48–53, 2017.

D. Abril, G. Navarro-Arribas, and V. Torra. Improving record linkage with supervised learning for disclosure risk assessment. *Information Fusion*, 13(4):274 – 284, 2012a.

D. Abril, G. Navarro-Arribas, and V. Torra. Choquet integral for record linkage. *Annals of Operations Research*, 195(1):97–110, 2012b.

A. K. Adams, A. J. Lee, and D. Mossé. Receipt-mode trust negotiation: efficient authorization through outsourced interactions. In *06th ACM Symposium on Information, Computer and Communications Security*, pages 430–434. ACM, 2011.

A. Agarwal. Limits on interconnection network performance. *IEEE Transactions on Parallel and Distributed Systems*, 2(4):398–412, 1991.

E. M. Airoldi, X. Bai, and B. A. Malin. An entropy approach to disclosure risk assessment: Lessons from real applications and simulated domains. *Decision Support Systems*, 51 (1):10–20, 2011.

O. Akan, O. Karli, and O. Ergul. Cognitive radio sensor networks. *IEEE Network*, 23(4): 34–40, July 2009.

O. B. Akan, V. C. Gungor, et al. Spectrum-aware and cognitive sensor networks for smart grid applications. *IEEE Communications Magazine*, 50(5):158–165, 2012.

F. Akhtar, M. H. Rehmani, and M. Reisslein. White space: Definitional perspectives and their role in exploiting spectrum opportunities. *Telecommunications Policy*, 40(4): 319–331, 2016.

I. F. Akyildiz and M. C. Vuran. *Wireless sensor networks*, volume 4. John Wiley & Sons, 2010.

I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE communications magazine*, 40(8):102–114, 2002.

I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer networks*, 50 (13):2127–2159, 2006.

I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. A survey on spectrum management in cognitive radio networks. *IEEE Communications Magazine*, 46(4):40–48, 2008.

I. F. Akyildiz, B. F. Lo, and R. Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: A survey. *Physical Communication*, 4(1):40–62, 2011.

M. Al Ameen, J. Liu, and K. Kwak. Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems*, 36(1):93–101, 2012.

K. A. Al Mamun, M. Alhussein, K. Sailunaz, and M. S. Islam. Cloud based framework for parkinsons disease diagnosis and monitoring system for remote healthcare applications. *Future Generation Computer Systems*, 66:36–47, 2017.

C. Alippi, G. Anastasi, M. Di Francesco, and M. Roveri. Energy management in wireless sensor networks with energy-hungry sensors. *IEEE Instrumentation & Measurement Magazine*, 12(2):16–23, 2009.

A. Almutairi, M. Sarfraz, S. Basalamah, W. Aref, and A. Ghafoor. A distributed access control architecture for cloud computing. *IEEE Software*, 29(2):36 – 44, 2012.

A. Anghel, G. Vasile, R. Boudon, G. dUrso, A. Girard, D. Boldo, and V. Bost. Combining spaceborne sar images with 3d point clouds for infrastructure monitoring applications. *ISPRS Journal of Photogrammetry and Remote Sensing*, 111:45–61, 2016.

L. Angrisani, S. DAntonio, M. Vadursi, and G. Ventre. Packet delay models in packet-switched networks: Performance assessment through capacity measurements. In *European Simulation and Modeling Conference*, pages 465–469. Citeseer, 2003.

L. Antal, N. Shlomo, and M. Elliot. Measuring disclosure risk with entropy in population based frequency tables. In *Privacy in Statistical Databases*, pages 62–78. Springer, 2014.

P. Arias-Cabarcos, F. Almenárez-Mendoza, A. Marín-López, D. Díaz-Sánchez, and R. Sánchez-Guerrero. A metric-based approach to assess risk for on cloud federated identity management. *Journal of Network and Systems Management*, 20(4):513–533, 2012a.

P. Arias-Cabarcos, F. Almenrez-Mendoza, A. Marn-Lpez, D. Daz-Snchez, and R. Snchez-Guerrero. A metric-based approach to assess risk for on cloud federated identity management. *Journal of Network and Systems Management*, 20(4):513–533, 2012b.

K. J. Arrow. The role of securities in the optimal allocation of risk-bearing. *The Review of Economic Studies*, 31(2):91–96, 1964.

L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, 2004.

E. Axell, G. Leus, E. G. Larsson, and H. V. Poor. Spectrum sensing for cognitive radio: State-of-the-art and recent advances. *IEEE Signal Processing Magazine*, 29(3):101–116, 2012.

R. B. Ayed, P. Bon, and S. Collart-Dutilleul. Checking the european railways traffic management system (ertms) operating rules using uml and b method. In *14th International conference on Railway Engineering Design and Optimization*, pages 139–149, 2014.

A. Azarfar, J.-F. Frigon, and B. Sansò. Delay analysis of multichannel opportunistic spectrum access mac protocols. *IEEE Transactions on Mobile Computing*, 15(1):92–106, 2016.

T. Bartkewitz. Building hash functions from block ciphers, their security and implementation properties. http://www.emsec.rub.de/media/crypto/attachments/files/2011/03/bartkewitz.pdf, 2009.

S. Bartsch. A calculus for the qualitative risk assessment of policy override authorization. In *03rd international conference on Security of information and networks*, pages 62–70. ACM, 2010.

S. Baselice, P. Bonatti, and M. Faella. On interoperable trust negotiation strategies. In *08th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07)*, pages 39–50, June 2007.

A. Bauer, M. Leucker, and C. Schallhart. Comparing ltl semantics for runtime verification. *Journal of Logic and Computation*, 20(3):651–674, 2010.

S. Bayhan and F. Alagoz. Scheduling in centralized cognitive radio networks for energy efficiency. *IEEE Transactions on Vehicular Technology*, 62(2):582–595, 2013.

N. D. Belnap Jr. A useful four-valued logic. In *Modern Uses of Multiple-valued Logic*, pages 5–37. Springer, 1977.

E. Bertino, F. Buccafurri, E. Ferrari, and P. Rullo. A logical framework for reasoning on data access control policies. In *12th IEEE Computer Security Foundations Workshop*, pages 175–189, 1999.

E. Bertino, E. Ferrari, and A. Squicciarini. Trust negotiations: concepts, systems, and languages. *Computing in Science & Engineering*, 6(4):27–34, 2004.

E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini. Digital identity management and trust negotiation. In *Security for Web Services and Service-Oriented Architectures*, pages 79–114. 2010.

J. G. Bethlehem, W. J. Keller, and J. Pannekoek. Disclosure control of microdata. *Journal of the American Statistical Association*, 85(409):38–45, 1990.

M. Bezzi. An entropy based method for measuring anonymity. In *03rd International Conference on Security and Privacy in Communications Networks and the Workshops*, pages 28–32. IEEE, 2007.

M. Bezzi. Expressing privacy metrics as one-symbol information. In *EDBT/ICDT Workshops*, EDBT '10, pages 29:1–29:5, 2010.

N. Bhalaji and C. Selvaraj. Comprehensive trust based scheme to combat malicious nodes in manet based cyber physical systems. In *Proceedings of International Conference on Communication and Networks*, pages 543–550. Springer, 2017.

A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino. Trust negotiation in identity management. *IEEE Security & Privacy*, 5(2):55 – 63, 2007.

A. O. Bicen, O. B. Akan, and V. C. Gungor. Spectrum-aware and cognitive sensor networks for smart grid applications. *IEEE Communications Magazine*, 50(5):158–165, 2012a.

A. O. Bicen, V. C. Gungor, and O. B. Akan. Delay-sensitive and multimedia communication in cognitive radio sensor networks. *Ad Hoc Networks*, 10(5):816–830, 2012b.

A. O. Bicen, E. B. Pehlivanoglu, S. Galmes, and O. B. Akan. Dedicated radio utilization for spectrum handoff and efficiency in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 14(9):5251–5259, 2015.

L. Bilge and T. Dumitras. Before we knew it: an empirical study of zero-day attacks in the real world. In *ACM conference on Computer and communications security*, pages 833–844, 2012.

E. Birrell and F. B. Schneider. Federated identity management systems: A privacy-based characterization. *IEEE Security & Privacy*, 11(5):36–48, 2013.

I. Bisio, F. Lavagetto, M. Marchese, and A. Sciarrone. Smartphone-centric ambient assisted living platform for patients suffering from co-morbidities monitoring. *IEEE Communications Magazine*, 53(1):34–41, 2015.

L. Bolotnyy and G. Robins. Physically unclonable function-based security and privacy in rfid systems. In *05th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07)*, pages 211–220. IEEE, 2007.

K. Bonne Rasmussen and S. Capkun. Implications of radio fingerprinting on the security of sensor networks. In *03rd International Conference on Security and Privacy in Communications Networks and the Workshops*, pages 331–340, Sept 2007.

F. Borgonovo, M. Cesana, and L. Fratta. Throughput and delay bounds for cognitive transmissions. In *Advances in Ad Hoc Networking*, pages 179–190. Springer, 2008.

R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and control*, 3(1):68–79, 1960.

J. A. Botia, A. Villa, and J. Palma. Ambient assisted living system for in-home monitoring of healthy independent elders. *Expert Systems with Applications*, 39(9):8136–8148, 2012.

A. Botta, W. De Donato, V. Persico, and A. Pescapé. Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, 56:684–700, 2016.

A. D. Brucker and H. Petritsch. Extending access control models with break-glass. In *14th ACM symposium on Access Control Models and Technologies*, pages 197–206. ACM, 2009.

A. D. Brucker, H. Petritsch, and S. G. Weber. Attribute-based encryption with break-glass. In *IFIP International Workshop on Information Security Theory and Practices*, pages 237–244. Springer, 2010.

M. Bruyneel and V. Ninane. Unattended home-based polysomnography for sleep disordered breathing: current concepts and perspectives. *Sleep Medicine Reviews*, 18(4): 341–347, 2014.

R. Buyya, R. Ranjan, and R. N. Calheiros. Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. In *International Conference on Algorithms and Architectures for Parallel Processing*, pages 13–31. Springer, 2010.

Y. Cai, Y. Mo, K. Ota, C. Luo, M. Dong, and L. Yang. Optimal data fusion of collaborative spectrum sensing under attack in cognitive radio networks. *IEEE Network*, 28(1):17–23, 2014.

B. Carminati, E. Ferrari, and M. Guglielmi. Secure information sharing on support of emergency management. In *IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and IEEE Third Inernational Conference on Social Computing (SocialCom)*, pages 988–995. IEEE, 2011.

B. Carminati, E. Ferrari, and M. Guglielmi. Controlled information sharing for unspecified emergencies. In *International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pages 1–8. IEEE, 2013.

F. Cerutti, L. M. Kaplan, T. J. Norman, N. Oren, and A. Toniolo. Subjective logic operators in trust assessment: an empirical study. *Information Systems Frontiers*, 17 (4):743–762, 2015.

D. W. Chadwick and G. Inman. The trusted attribute aggregation service (taas)-providing an attribute aggregation layer for federated identity management. In *08th International Conference on Availability, Reliability and Security (ARES)*, pages 285–290. IEEE, 2013.

R. K. Chahal and S. Singh. Fuzzy rule-based expert system for determining trustworthiness of cloud service providers. *International Journal of Fuzzy Systems*, pages 1–17, 2016.

R. Chai, Z. Guo, and Q. Hu. Total transmission delay minimization based spectrum selection scheme for heterogeneous cognitive radio networks. In *IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, pages 1862–1866. IEEE, 2014.

S. Chakraborty, Z. Charbiwala, H. Choi, K. R. Raghavan, and M. B. Srivastava. Balancing behavioral privacy and information utility in sensory data flows. *Pervasive and Mobile Computing*, 8(3):331–345, 2012.

J.-H. Chang and L. Tassiulas. Maximum lifetime routing in wireless sensor networks. *IEEE/ACM Transactions on Networking*, 12(4):609–619, 2004.

S. Chatterjee and P. S. Chatterjee. A comparison based clustering algorithm to counter ssdf attack in cwsn. In *International Conference on Computational Intelligence and Networks (CINE)*, pages 194–195. IEEE, 2015.

L. Chen and J. Crampton. Risk-aware role-based access control. In *Security and Trust Management*, pages 140–156. Springer, 2012.

T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford. Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on Smart Grid*, 2(4):741–749, 2011.

P. Cheng, R. Deng, and J. Chen. Energy-efficient cooperative spectrum sensing in sensor-aided cognitive radio networks. *IEEE Wireless Communications*, 19(6):100–105, 2012.

P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger. Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In *IEEE Symposium on Security and Privacy*, pages 222–230. IEEE, 2007.

A. Chonka, Y. Xiang, W. Zhou, and A. Bonti. Cloud security defence to protect cloud computing against http-dos and xml-dos attacks. *Journal of Network and Computer Applications*, 34(4):1097–1107, 2011.

S. S. Chow, Y.-J. He, L. C. Hui, and S. M. Yiu. Spice–simple privacy-preserving identity-management for cloud environment. In *Applied Cryptography and Network Security*, pages 526–543. Springer, 2012.

S. D. Chowdhury, G. T. Duncan, R. Krishnan, S. F. Roehrig, and S. Mukherjee. Disclosure detection in multivariate categorical databases: Auditing confidentiality protection through two new matrix operators. *Management Science*, 45(12):1710–1723, 1999.

J. V. Cleemput, B. Coppens, and B. De Sutter. Compiler mitigations for time attacks on modern x86 processors. *ACM Transactions on Architecture and Code Optimization (TACO)*, 8(4):23, 2012.

D. R. Cox. *Renewal theory*, volume 58. Methuen, 1962.

P. Cox. How to manage identity in the public cloud. http://reports.informationweek.com/abstract/21/8691/ security/strategy-how-to-manage-identity-in-the-public-cloud.html, 2012.

K. Crawford and M. Finn. The limits of crisis data: analytical and ethical challenges of using social and mobile data to understand disasters. *GeoJournal*, 80(4):491–502, 2015.

Cummins. http://power.cummins.com/remote-monitoring, 2017. Accessed information in February 2017.

B. Cusack and E. Ghazizadeh. Analysing trust issues in cloud identity environments, 2016. Accessed from:http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1042&context=acis2016.

CVE. Common vulnerabilities and exposures (cve). http://cve.mitre.org/cve/cve.html, 2014.

M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca. Geo-rbac: A spatially aware rbac. *ACM Transactions on Information and System Security (TISSEC)*, 10(1):2, 2007.

R. A. Dandekar, J. Domingo-Ferrer, and F. Sebé. Lhs-based hybrid microdata vs rank swapping and microaggregation for numeric microdata protection. In *Inference Control in Statistical Databases*, pages 153–162. Springer, 2002.

A. Das and M. M. Islam. Securedtrust: a dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing*, 9(2):261–274, 2012.

A. Dastjerdi and R. Buyya. Compatibility-aware cloud service composition under fuzzy preferences of users. *IEEE Transactions on Cloud Computing*, 2(1):1–13, Jan 2014.

J. Delvaux and I. Verbauwhede. Attacking puf-based pattern matching key generators via helper data manipulation. In *Topics in Cryptology CT-RSA 2014*, volume 8366 of *Lecture Notes in Computer Science*, pages 106–131. Springer International Publishing, 2014.

R. Deng, J. Chen, C. Yuen, P. Cheng, and Y. Sun. Energy-efficient cooperative spectrum sensing by optimal scheduling in sensor-aided cognitive radio networks. *IEEE Transactions on Vehicular Technology*, 61(2):716–725, 2012.

S. Deng, L. Huang, J. Taheri, and A. Y. Zomaya. Computation offloading for service workflow in mobile cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, 26(12):3317–3329, 2015.

S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal. Design and implementation of PUF-based ünclonable" RFID ICs for anti-counterfeiting and security applications. In *IEEE International Conference on RFID*, pages 58–64. IEEE, 2008.

A. K. Dey. Understanding and using context. *Personal and ubiquitous computing*, 5(1): 4–7, 2001.

N. Dimmock, A. Belokosztolszki, D. Eyers, J. Bacon, and K. Moody. Using trust and risk in role-based access control policies. In *09th ACM symposium on Access Control Models and Technologies*, pages 156–162. ACM, 2004.

S. Ding and L. Liu. A node-disjoint multipath routing protocol based on aodv. In *Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science*, pages 312–316. IEEE, 2010.

A. Dobra, S. E. Fienberg, A. Rinaldo, A. Slavkovic, and Y. Zhou. Algebraic statistics and contingency table problems: Log-linear models, likelihood estimation, and disclosure limitation. In *Emerging Applications of Algebraic Geometry*, pages 63–88. Springer, 2009.

J. Domingo-Feffer, A. Oganian, and V. Torra. Information-theoretic disclosure risk measures in statistical disclosure control of tabular data. In *14th International Conference on Scientific and Statistical Database Management*, pages 227–231. IEEE, 2002.

J. Domingo-Ferrer and J. M. Mateo-Sanz. Practical data-oriented microaggregation for statistical disclosure control. *IEEE Transactions on Knowledge and Data Engineering*, 14(1):189–201, 2002.

J. Domingo-Ferrer, J. M. Mateo-Sanz, and V. Torra. Comparing sdc methods for microdata on the basis of information loss and disclosure risk. In *Pre-proceedings of ETK-NTTS*, volume 2, pages 807–826, 2001.

M. G. Dondo. A vulnerability prioritization system using a fuzzy risk analysis approach. In *IFIP International Information Security Conference*, pages 525–540. Springer, 2008.

D. R. Dos Santos, C. M. Westphall, and C. B. Westphall. A dynamic risk-based access control architecture for cloud computing. In *Network Operations and Management Symposium (NOMS)*, pages 1–9. IEEE, 2014.

G. Dreo, M. Golling, W. Hommel, and F. Tietze. Iceman: An architecture for secure federated inter-cloud identity management. In *IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*, pages 1207–1210. IEEE, 2013.

L. Duan, A. W. Min, J. Huang, and K. G. Shin. Attack prevention for collaborative spectrum sensing in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 30(9):1658–1665, 2012.

G. Duncan, M. Elliot, and J.-J. Salazar-Gonzalez. Assessment of disclosure risk. In *Statistical Confidentiality*, Statistics for Social and Behavioral Sciences, pages 49–64. Springer New York, 2011. ISBN 978-1-4419-7801-1.

J. Dutta and S. Roy. Iot-fog-cloud based architecture for smart city: Prototype of a smart building. In *Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on*, pages 237–242. IEEE, 2017.

K. El Emam, E. Jonker, L. Arbuckle, and B. Malin. A systematic review of re-identification attacks on health data. *PloS one*, 6(12):e28071, 2011.

C. Emig, F. Brandt, S. Kreuzer, and S. Abeck. Identity as a service–towards a service-oriented identity management architecture. In *Dependable and Adaptable Networks and Services*, pages 1–8. Springer, 2007.

M. Ettus. System capacity, latency, and power consumption in multihop-routed ss-cdma wireless networks. In *IEEE Radio and Wireless Conference (RAWCON)*, pages 55–58. IEEE, 1998.

FCC. Et docket no 03-222 notice of proposed rule making and order, December 2003.

D. Feng, C. Jiang, G. Lim, L. J. Cimini, G. Feng, and G. Y. Li. A survey of energy-efficient wireless communications. *IEEE Communications Surveys & Tutorials*, 15(1):167–178, 2013.

J. Feng, M. Wang, G. Lu, and J. Li. Trusted cooperative spectrum sensing scheme based on ds evidence theory. In *International Conference on Information and Communications Technologies (ICT 2015)*, pages 1–5. IET, 2015.

S. Feng, Z. Liang, and D. Zhao. Providing telemedicine services in an infrastructure-based cognitive radio network. *IEEE Wireless Communications*, 17(1):96–103, 2010.

D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio. Security issues in cloud environments: a survey. *International Journal of Information Security*, 13(2):113–170, 2014.

A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zao, R. Chilro, and L. Antunes. How to securely break into rbac: the btg-rbac model. In *Annual Computer Security Applications Conference (ACSAC'09)*, pages 23–31. IEEE, 2009.

S. E. Fienberg. Fréchet and bonferroni bounds for multi-way tables of counts with applications to disclosure limitation. In *Proceedings of Statistical Data Protection (SDP98)*, pages 115–129, 1999.

S. E. Fienberg and A. B. Slavkovic. Preserving the confidentiality of categorical statistical data bases when releasing information for association rules. *Data Mining and Knowledge Discovery*, 11(2):155–180, 2005.

A. Filieri, C. Ghezzi, and G. Tamburrelli. Run-time efficient probabilistic model checking. In *Proceedings of the 33rd international conference on software engineering*, pages 341–350. ACM, 2011.

J. Freudiger, R. Shokri, and J.-P. Hubaux. Evaluating the privacy risk of location-based services. In *Financial Cryptography*, volume 7035, pages 31–46. Springer, 2011.

M. Fugini, M. Teimourikia, and G. Hadjichristofi. A web-based cooperative tool for risk management with adaptive security. *Future Generation Computer Systems*, 54:409–422, 2016.

S. R. Gandham, M. Dawande, R. Prakash, and S. Venkatesan. Energy efficient schemes for wireless sensor networks with multiple mobile base stations. In *Global telecommunications conference. GLOBECOM'03*, volume 1, pages 377–381. IEEE, 2003.

Y. Gao, H. Ma, D. C. Ranasinghe, S. F. Al-Sarawi, and D. Abbott. Exploiting puf unreliability to secure wireless sensing. *IEEE Transactions in Circuits and Systems I:Regular Papers*, PP:1–12, 2017.

L. Gasparini. Risk-aware access control and xacml. http://tesi.cab.unipd.it/42991/, 2013.

E. Georgakakis, S. A. Nikolidakis, D. D. Vergados, and C. Douligeris. Spatio temporal emergency role based access control (stem-rbac): a time and location aware role based access control model with a break the glass mechanism. In *IEEE Symposium on Computers and Communications (ISCC)*, pages 764–770. IEEE, 2011.

E. Ghazizadeh, J.-l. A. Manan, M. Zamani, and A. Pashang. A survey on security issues of federated identity in the cloud computing. In *04th International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 532–565. IEEE, 2012.

N. Ghosh, S. K. Ghosh, and S. K. Das. Selcsp: A framework to facilitate selection of cloud service providers. *IEEE transactions on Cloud Computing*, 3(1):66–79, 2015.

D. Giannakopoulou and K. Havelund. Automata-based verification of temporal properties on running programs. In *16th Annual International Conference on Automated Software Engineering (ASE 2001)*, pages 412–416. IEEE, 2001.

M. Godfrey and M. Zulkernine. A server-side solution to cache-based side-channel attacks in the cloud. In *06th IEEE International Conference on Cloud Computing*, pages 163–170, 2013.

A. J. Goldsmith and P. P. Varaiya. Capacity of fading channels with channel side information. *IEEE Transactions on Information Theory*, 43(6):1986–1992, 1997.

A. Gopalakrishnan. Cloud computing identity management. *SETLabs briefings*, 7(7): 45–54, 2009.

B. Green, M. Krotofil, and D. Hutchison. Achieving ics resilience and security through granular data flow management. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, pages 93–101. ACM, 2016.

G. Grieco, G. L. Grinblat, L. Uzal, S. Rawat, J. Feist, and L. Mounier. Toward large-scale vulnerability discovery using machine learning. In *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, pages 85–96. ACM, 2016.

N. Gruschka and M. Jensen. Attack surfaces: A taxonomy for attacks on cloud services. In *03rd IEEE International Conference on Cloud Computing*, pages 276–279, 2010.

J. Guajardo, S. S. Kumar, and P. Tuyls. Key distribution for wireless sensor networks and physical unclonable functions. *Printed handout of Secure Component and System IdentificationSECSI*, pages 17–18, 2008.

J. Guajardo, B. Škorić, P. Tuyls, S. S. Kumar, T. Bel, A. H. Blom, and G.-J. Schrijen. Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. *Information Systems Frontiers*, 11(1):19–41, 2009.

J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29 (7):1645–1660, 2013.

D. Gunduz, K. Stamatiou, N. Michelusi, and M. Zorzi. Designing intelligent energy harvesting communication systems. *IEEE Communications Magazine*, 52(1):210–216, 2014.

V. C. Gungor and F. C. Lambert. A survey on communication networks for electric system automation. *Computer Networks*, 50(7):877–897, 2006.

V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke. A survey on smart grid potential applications and communication requirements. *IEEE Transactions on Industrial Informatics*, 9(1):28–42, 2013.

C. Guo, T. Peng, S. Xu, H. Wang, and W. Wang. Cooperative spectrum sensing with cluster-based architecture in cognitive radio networks. In *69th IEEE Vehicular Technology Conference, VTC Spring*, pages 1–5. IEEE, 2009.

W. Guo, S. Chen, Y. Guo, L. Luo, and Z. Zhao. Truster: Trusted social behavior inspired scheme for cooperative spectrum sensing. In *16th International Conference on Communication Technology (ICCT)*, pages 583–588. IEEE, 2015.

S. K. S. Gupta, T. Mukheriee, K. Venkatasubramanian, and T. B. Taylor. Proximity based access control in smart-emergency departments. In *04th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 5 pp.–516, March 2006.

S. M. Habib, S. Ries, M. Mühlhäuser, and P. Varikkattu. Towards a trust management system for cloud computing marketplaces: using caiq as a trust information source. *Security and Communication Networks*, 2013.

I. Haider, M. Höberl, and B. Rinner. Trusted sensors for participatory sensing and iot applications based on physically unclonable functions. In *02nd ACM International Workshop on IoT Privacy, Trust, and Security*, pages 14–21. ACM, 2016.

G. Han, L. Liu, J. Jiang, L. Shu, and G. Hancke. Analysis of energy-efficient connected target coverage algorithms for industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 13(1):135–143, 2017.

Y. Han, S. H. Ting, and A. Pandharipande. Cooperative spectrum sharing with distributed secondary user selection. In *IEEE International Conference on Communications (ICC)*, pages 1–5. IEEE, 2010.

A. Harel, A. Shabati, L. Rokach, and Y. Elovici. Dynamic sensitivity-based access control. pages 201–203, 2010.

S. Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, 23(2):201–220, 2005.

K. Henricksen, J. Indulska, and A. Rakotonirainy. Modeling context information in pervasive computing systems. In *International Conference on Pervasive Computing*, pages 167–180. Springer, 2002.

K. Henry and D. Stinson. Secure network discovery in wireless sensor networks using combinatorial key pre-distribution. In *Workshop on Lightweight Security Privacy: Devices, Protocols and Applications (LightSec),*, pages 34–43, March 2011.

C. Herald. Power restored to downtown calgary five days after outage. http://live.calgaryherald. com/Event/ Part_of_downtown_Calgary _in_darkness_after _underground_ electrical_fire?Page=0, 2014. Accessed on 16th January 2015.

C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, 102(8):1126–1141, 2014.

D. T. Hoang, D. Niyato, P. Wang, and D. I. Kim. Opportunistic channel access and rf energy harvesting in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 32(11):2039–2052, 2014.

G. Holmes, A. Donkin, and I. H. Witten. Weka: A machine learning workbench. In *02nd Australian and Nw Zealand Conference on Intelligent Information Systems*, pages 357 – 361. IEEE, 1994.

E. Horvitz. Transmission and display of information for time-critical decisions, 1995.

A. Høyland and M. Rausand. *System Reliability Theory: Models and Statistical Methods*, volume 420. John Wiley & Sons, 2009.

H. Hu, H. Zhang, H. Yu, Y. Xu, and N. Li. Minimum transmission delay via spectrum sensing in cognitive radio networks. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 4101–4106. IEEE, 2013.

A. Hundepool, J. Domingo-Ferrer, L. Franconi, S. Giessing, E. S. Nordholt, K. Spicer, and P.-P. De Wolf. *Statistical disclosure control*. John Wiley & Sons, 2012.

C. S. Hyder, B. Grebur, and L. Xiao. Defense against spectrum sensing data falsification attacks in cognitive radio networks. In *Security and privacy in communication networks*, pages 154–171. Springer, 2012.

C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison. Arc: Adaptive reputation based clustering against spectrum sensing data falsification attacks. *IEEE Transactions on Mobile Computing*, 13(8):1707–1719, 2014.

J. Idziorek, M. F. Tannian, and D. Jacobson. The insecurity of cloud utility models. *IT Professional*, 15(2):22–27, 2013. ISSN 1520-9202. doi: http://doi.ieeecomputersociety.org/10.1109/MITP.2012.43.

I. Immoreev and S. Ivashov. Remote monitoring of human cardiorespiratory system parameters by radar and its applications. In *Ultrawideband and Ultrashort Impulse Signals, 2008. UWBUSIS 2008. 4th International Conference on*, pages 34–38. IEEE, 2008.

A. in Cyber Systems and T. G. of MIT. http://www.ll.mit.edu/mission/communications/cyber/CSTcorpo /ideval/data/index.html, 2000. Data downloaded on 16-08-2014.

ISO8402. Quality management and quality assurance - vocabulary, 1994.

S. Jajodia, P. Samarati, and V. Subrahmanian. A logical language for expressing authorizations. In *IEEE Symposium on Security and Privacy*, pages 31–42, May 1997.

D. Jaramillo, N. Katz, B. Bodin, W. Tworek, R. Smart, and T. Cook. Cooperative solutions for bring your own device (byod). *IBM Journal of Research and Development*, 57(6):5:1–5:11, Nov 2013.

J. Jensen. Federated identity management challenges. In *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, pages 230–235. IEEE, 2012.

R. Jensen and Q. Shen. Fuzzy-rough sets for descriptive dimensionality reduction. In *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE'02)*, volume 1, pages 29–34, 2002.

X. Jin, R. Sandhu, and R. Krishnan. Rabac: role-centric attribute-based access control. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, pages 84–96. Springer, 2012.

E. Jonsson and T. Olovsson. A quantitative model of the security intrusion process based on attacker behavior. *IEEE Transactions on Software Engineering*, 23(4):235–245, 1997.

A. Jøsang, R. Hayward, and S. Pope. Trust network analysis with subjective logic. In *Proceedings of the 29th Australasian Computer Science Conference-Volume 48*, pages 85–94. Australian Computer Society, Inc., 2006.

A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2):618–644, 2007.

C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, 1(2):293–315, 2003.

R. L. Keeney. Utility functions for multiattributed consequences. *Management Science*, 18(5-part-1):276–287, 1972.

R. L. Keeney. Multiplicative utility functions. *Operations Research*, 22(1):22–34, 1974.

C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni. T-vnets: A novel trust architecture for vehicular networks using the standardized messaging services of etsi its. *Computer Communications*, 93:68–83, 2016.

A. A. Khan, M. H. Rehmani, and M. Reisslein. Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols. *IEEE Communications Surveys & Tutorials*, 18(1):860–898, 2016.

M. Kim, J. Ryou, Y. Choi, and S. Jun. Low-cost cryptographic circuits for authentication in radio frequency identification systems. In *Tenth International Symposium on Consumer Electronics*, pages 1–5. IEEE, 2006.

A. Kinalis, S. Nikoletseas, D. Patroumpa, and J. Rolim. Biased sink mobility with adaptive stop times for low latency data collection in sensor networks. *Information Fusion*, 15: 56–63, 2014.

M. S. Kirkpatrick, G. Ghinita, and E. Bertino. Privacy-preserving enforcement of spatially aware rbac. *IEEE Transactions on Dependable and Secure Computing*, 9(5):627–640, 2012.

R. Kissel. Glossary of key information security terms. *NIST Interagency Reports NIST IR*, 7298(3), 2013.

R. Klauck, J. Gaebler, M. Kirsche, and S. Schoepke. Mobile xmpp and cloud service collaboration: An alliance for flexible disaster management. In *17th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, pages 201–210. IEEE, 2011.

S. Kleber, F. Unterstein, M. Matousek, F. Kargl, F. Slomka, and M. Hiller. Secure execution architecture based on puf-driven instruction level code encryption. *IACR Cryptology ePrint Archive*, 2015:651, 2015.

T. Kleinberger, A. Jedlitschka, H. Storf, S. Steinbach-Nordmann, and S. Prueckner. An approach to and evaluations of assisted living systems using ambient intelligence for

emergency monitoring and prevention. In *International Conference on Universal Access in Human-Computer Interaction*, pages 199–208. Springer, 2009.

D. A. Knox and T. Kunz. Practical rf fingerprints for wireless sensor network authentication. In *08th International Wireless Communications and Mobile Computing Conference (IWCMC),*, pages 531–536, Aug 2012.

J. Kohlrausch. Experiences with the noah honeynet testbed to detect new internet worms. In *Fifth International Conference on IT Security Incident Management and IT Forensics (IMF'09)*, pages 13–26. IEEE, 2009.

G. Kokolakis and P. Nanopoulos. Bayesian multivariate micro-aggregation under the hellingers distance criterion. *Research in Official Statistics*, 4(1):117–126, 2001.

I. Korhonen, J. Pärkkä, and M. Van Gils. Health monitoring in the home of the future. *IEEE Engineering in Medicine and Biology Magazine*, 22(3):66–73, 2003.

I. V. Kotenko and E. Doynikova. Evaluation of computer network security based on attack graphs and security event processing. *JoWUA*, 5(3):14–29, 2014.

D. Kotz. A threat taxonomy for mhealth privacy. In *COMSNETS*, pages 1–6, 2011.

F. J. Krautheim, D. S. Phatak, and A. T. Sherman. Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing. In *Trust and Trustworthy Computing*, pages 211–227. Springer, 2010.

D. R. Kuhn, E. J. Coyne, and T. R. Weil. Adding attributes to role-based access control. *IEEE Computer*, 43(6):79–81, 2010.

H. W. Kuhn. The hungarian method for the assignment problem. In *50 Years of Integer Programming 1958-2008*, pages 29–47. Springer, 2010.

D. Kulkarni and A. Tripathi. Context-aware role-based access control in pervasive computing systems. In *13th ACM symposium on Access control models and technologies*, pages 113–122. ACM, 2008.

K. Kursawe, A. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls. Reconfigurable physical unclonable functions-enabling technology for tamper-resistant storage. In *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'09)*, pages 22–29. IEEE, 2009.

V. M. Kuthadi, R. Selvaraj, and T. Marwala. An enhanced security pattern for wireless sensor network. In *Proceedings of the Second International Conference on Computer and Communication Technologies*, pages 61–71. Springer, 2016.

Y. Kwon, D. K. Park, and H. Rhee. Spectrum fragmentation: Causes, measures and applications. *Telecommunications Policy*, 41(56):447–459, 2017.

D.-J. Lee. Adaptive random access for cooperative spectrum sensing in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 14(2):831–840, 2015.

Y. S. Lee, H. J. Lee, and E. Alasaarela. Mutual authentication in wireless body sensor networks (wbsn) based on physical unclonable function (puf). In *09th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 1314–1318. IEEE, 2013.

A. Leon-Garcia. *Probability and Random Processes for Electrical Engineering.* 2004.

H. Li, X. Xing, J. Zhu, X. Cheng, K. Li, R. Bie, and T. Jing. Utility-based cooperative spectrum sensing scheduling in cognitive radio networks. *IEEE Transactions on Vehicular Technology*, 66(1):645–655, 2017.

N. Li, T. Li, and S. Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In *23rd IEEE International Conference on Data Engineering*, pages 106–115. IEEE, 2007.

Q. Li and W. Ba. A group priority earliest deadline first scheduling algorithm. *Frontiers of Computer Science*, 6(5):560–567, 2012.

T. Li, J. Ren, and X. Tang. Secure wireless monitoring and control systems for smart grid and smart home. *IEEE Wireless Communications*, 19(3):66–73, 2012a.

W. Li, A. Joshi, and T. Finin. Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach. In *11th International Conference on Mobile Data Management*, pages 85–94. IEEE, 2010.

X. Li and J. Du. Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing. *IET Information Security*, 7(1):39–50, 2013.

Y. Li, S. K. Jayaweera, M. Bkassiny, and K. A. Avery. Optimal myopic sensing and dynamic spectrum access in cognitive radio networks with low-complexity implementations. *IEEE Transactions on Wireless Communications*, 11(7):2412–2423, 2012b.

X. Liang, X. Li, M. Barua, L. Chen, R. Lu, X. Shen, and H. Luo. Enable pervasive healthcare through continuous remote health monitoring. *IEEE Wireless Communications*, 19(6):10–18, 2012.

J. Liebeherr, D. E. Wrege, and D. Ferrari. Exact admission control for networks with a bounded delay service. *IEEE/ACM Transactions on Networking (TON)*, 4(6):885–901, 1996.

L. Lin, D. Holcomb, D. K. Krishnappa, P. Shabadi, and W. Burleson. Low-power subthreshold design of secure physical unclonable functions. In *Proceedings of the 16th ACM/IEEE international symposium on Low power electronics and design*, pages 43–48. ACM, 2010.

A. Liu, J. Ren, X. Li, Z. Chen, and X. S. Shen. Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks. *Computer Networks*, 56(7):1951–1967, 2012.

G. Liu, R. Zhang, H. Song, C. Wang, J. Liu, and A. Liu. Ts-rbac: A rbac model with transformation. *Computers & Security*, 60:52–61, 2016.

L. Liu. From data privacy to location privacy: models and algorithms. In *Proceedings of the 33rd international conference on Very large data bases*, pages 1429–1430. VLDB Endowment, 2007.

Q. Liu, X. Wang, and Y. Cui. Scheduling of sequential periodic sensing for cognitive radios. In *Proceedings of INFOCOM*, pages 2256–2264. IEEE, 2013.

F. Lombardi and R. Di Pietro. Secure virtualization for cloud computing. *Journal of Network and Computer Applications*, 34(4):1113–1122, 2011.

B. Lu and V. C. Gungor. Online and remote motor energy monitoring and fault diagnostics using wireless sensor networks. *IEEE Transactions on Industrial Electronics*, 56(11): 4651–4659, 2009.

X. Luo, H. Li, J. Zhang, and J. Shim. Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision support systems*, 49(2):222–234, 2010.

H. Ma, L. Zheng, X. Ma, and Y. Iuo. Spectrum aware routing for multi-hop cognitive radio networks with a single transceiver. In *03rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pages 1–6. IEEE, 2008.

R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng. Smart grid communication: Its challenges and opportunities. *IEEE Transactions on Smart Grid*, 4(1):36–46, 2013.

A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam. L-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data*, 1 (1), 2007.

R. Maes and I. Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security*, pages 3–37. Springer, 2010.

C. Mahapatra, P. Kamalinejad, T. Stouraitis, S. Mirabbasi, and V. C. Leung. Low-complexity energy-efficient security approach for e-health applications based on physically unclonable functions of sensors. In *International Conference on Electronics, Circuits, and Systems (ICECS)*, pages 531–534. IEEE, 2015.

G. Mahoney, W. J. Myrvold, and G. C. Shoja. Generic reliability trust model. In *PST*, volume 5, pages 113–120. Citeseer, 2005.

A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson. Wireless sensor networks for habitat monitoring. In *01st ACM International Workshop on Wireless Sensor Networks and Applications*, pages 88–97. ACM, 2002.

M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas. Slender puf protocol: A lightweight, robust, and secure authentication by substring matching. In *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on*, pages 33–44. IEEE, 2012.

A. C. Malady and C. R. da Silva. Clustering methods for distributed spectrum sensing in cognitive radio systems. In *IEEE Military Communications Conference (MILCOM)*, pages 1–5. IEEE, 2008.

E. Maler and D. Reed. The venn of identity: Options and issues in federated identity management. *IEEE Security & Privacy*, (2):16–23, 2008.

G. Mali and S. Misra. Trast: Trust-based distributed topology management for wireless multimedia sensor networks. *IEEE Transactions on Computers*, 65(6):1978–1991, 2016.

D. Manrique-Vallier and J. P. Reiter. Estimating identification disclosure risk using mixed membership models. *Journal of the American Statistical Association*, 107(500):1385–1394, 2012.

D. Margaria, E. Falletti, and T. Acarman. The need for gnss position integrity and authentication in its: Conceptual and practical limitations in urban contexts. In *IEEE Intelligent Vehicles Symposium*, pages 1384–1389. IEEE, 2014.

S. Marinovic, N. Dulay, and M. Sloman. Rumpole: An introspective break-glass access control language. *ACM Transactions on Information and System Security (TISSEC)*, 17(1):2, 2014.

S. P. Marsh. Formalising trust as a computational concept. 1994.

M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel. Time-to-compromise model for cyber risk reduction estimation. In *02nd ACM workshop on Quality of Protection*, pages 49–64. Springer, 2006.

S. Meguerdichian and M. Potkonjak. Device aging-based physically unclonable functions. In *48th Design Automation Conference*, pages 288–289. ACM, 2011a.

S. Meguerdichian and M. Potkonjak. Matched public puf: ultra low energy security platform. In *17th IEEE/ACM International Symposium on Low-power Electronics and Design*, pages 45–50. IEEE Press, 2011b.

K. W. Miller, J. M. Voas, and G. F. Hurlburt. Byod: Security and privacy considerations. *IT Professional*, 14(5):53–55, 2012.

E. L. Millner and M. D. Pratt. Risk aversion and rent-seeking: An extension and some experimental evidence. *Public Choice*, 69(1):81–92, 1991.

B.-C. Min, E. T. Matson, A. Smith, and J. E. Dietz. Using directional antennas as sensors to assist fire-fighting robots in large scale fires. In *Sensors Applications Symposium (SAS)*, pages 360–365. IEEE, 2014.

S. M. Mishra, A. Sahai, and R. W. Brodersen. Cooperative sensing among cognitive radios. In *International Conference on Communications (ICC)*, volume 4, pages 1658–1663. IEEE, 2006.

J. Mitola and G. Q. Maguire. Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 6(4):13–18, 1999.

A. K. Mok. Fundamental design problems of distributed systems for the hard-real-time environment. 1983.

I. Molloy, P.-C. Cheng, and P. Rohatgi. Trading in risk: Using markets to improve access control. In *Workshop on New Security Paradigms*, pages 107–125. ACM, 2009.

I. S. Moreno, P. Garraghan, P. Townend, and J. Xu. Analysis, modeling and simulation of workload patterns in a large-scale utility cloud. *IEEE Transactions on Cloud Computing*, 2(2):208–221, 2014.

R. A. Moser and G. Tardos. A constructive proof of the general lovász local lemma. *Journal of the ACM (JACM)*, 57(2):11, 2010.

Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle. Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey. *IEEE Communications Surveys & Tutorials*, 18(2):1287–1309, 2016.

A. Nagarajan and V. Varadharajan. Dynamic trust enhanced security model for trusted platform based services. *Future Generation Computer Systems*, 27(5):564 – 573, 2011.

M. Najimi, A. Ebrahimzadeh, S. M. H. Andargoli, and A. Fallahi. A novel sensing nodes and decision node selection method for energy efficiency of cooperative spectrum sensing in cognitive sensor networks. *IEEE Sensors Journal*, 13(5):1610–1621, 2013.

Netbiter. Remote management for power generators - https://www.lcautomation.com/wb˙documents/hms/netbiter%20remote%20management %20for Accessed information in February 2017.

S. D. Nguyen, T.-L. Pham, and D.-S. Kim. Dynamic spectrum handoff for industrial cognitive wireless sensor networks. In *11th IEEE International Conference on Industrial Informatics (INDIN)*, pages 92–97. IEEE, 2013.

J. Nin, J. Herranz, and V. Torra. Using classification methods to evaluate attribute disclosure risk. In *Modeling Decisions for Artificial Intelligence*, volume 6408 of *Lecture Notes in Computer Science*, pages 277–286. Springer Berlin Heidelberg, 2010.

D. Niyato, Q. Dong, P. Wang, and E. Hossain. Optimizations of power consumption and supply in the smart grid: Analysis of the impact of data communication reliability. *IEEE Transactions on Smart Grid*, 4(1):21–35, 2013.

T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu. Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Surveys*, 46(1):12:1–12:30, 2013. ISSN 0360-0300.

S.-H. Oh and S.-M. Yang. A modified least-laxity-first scheduling algorithm for real-time tasks. In *05th International Conference on Real-Time Computing Systems and Applications*, pages 31–36. IEEE, 1998.

C.-S. Ok, S. Lee, P. Mitra, and S. Kumara. Distributed energy balanced routing for wireless sensor networks. *Computers & Industrial Engineering*, 57(1):125–135, 2009.

M. Oto and O. Akan. Energy-efficient packet size optimization for cognitive radio sensor networks. *IEEE Transactions on Wireless Communications*, 11(4):1544–1553, April 2012.

J. Pacheco, C. Tunc, P. Satam, and S. Hariri. Secure and resilient cloud services for enhanced living environments. *IEEE Cloud Computing*, 3(6):44–52, 2016.

M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid. Internet of things in the 5g era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications*, 34(3):510–527, 2016.

J. Pamula, S. Jajodia, P. Ammann, and V. Swarup. A weakest-adversary security metric for network configuration security analysis. In *02nd ACM workshop on Quality of Protection*, pages 31–38. ACM, 2006.

S. Pandey, W. Voorsluys, S. Niu, A. Khandoker, and R. Buyya. An autonomic cloud environment for hosting ecg data analysis services. *Future Generation Computer Systems*, 28(1):147–154, 2012.

A. Pantelopoulos and N. G. Bourbakis. A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 40(1):1–12, 2010.

Z. Paral and S. Devadas. Reliable and efficient puf-based key generation using pattern matching. In *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 128–133, June 2011.

H. Pardue, J. Landry, and A. Yasinsac. A risk assessment model for voting systems using threat trees and monte carlo simulation. In *Requirements Engineering for e-Voting Systems (RE-VOTE), 2009 First International Workshop on*, pages 55–60. IEEE, 2010.

S. Park, J. Heo, B. Kim, W. Chung, H. Wang, and D. Hong. Optimal mode selection for cognitive radio sensor networks with rf energy harvesting. In *23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, pages 2155–2159. IEEE, 2012.

S. Pearson and M. Casassa-Mont. Sticky policies: an approach for managing privacy across multiple parties. *Computer*, 44(9):60–68, 2011.

E. Peh and Y.-C. Liang. Optimization for cooperative sensing in cognitive radio networks. In *Wireless Communications and Networking Conference,*, pages 27–32. IEEE, 2007.

M. Pesic, H. Schonenberg, and W. M. van der Aalst. Declare: Full support for loosely-structured processes. In *11th IEEE International Enterprise Distributed Object Computing Conference*, pages 287–287. IEEE, 2007.

J. Petäjäjärvi, K. Mikhaylov, M. Hämäläinen, and J. Iinatti. Evaluation of lora lpwan technology for remote health and wellbeing monitoring. In *Medical Information and Communication Technology (ISMICT), 2016 10th International Symposium on*, pages 1–5. IEEE, 2016.

H. Petritsch. A generic break-glass model. In *Break-Glass*, pages 37–50. Springer, 2014.

H. N. Pham, Y. Zhang, P. E. Engelstad, T. Skeie, and F. Eliassen. Optimal cooperative spectrum sensing in cognitive sensor networks. In *International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, pages 1073–1079. ACM, 2009.

V. Popescu, M. Fadda, and M. Murroni. Performance analysis of IEEE 802.22 wireless regional area network in the presence of digital video broadcasting–second generation terrestrial broadcasting services. *IET Communications*, 10(8):922–928, 2016.

U. Premarathne, I. Khalil, Z. Tari, and A. Zomaya. Cloud-based utility service framework for trust negotiations using federated identity management. *IEEE Transactions on Cloud Computing*, PP(99):1–1, 2015a.

U. S. Premarathne. Reliability analysis of trust based federated identity management in intercloud: A graph coloring approach. In *Consumer Communications & Networking Conference (CCNC), 2017 14th IEEE Annual*, pages 345–348. IEEE, 2017.

U. S. Premarathne, I. Khalil, and M. Atiquzzaman. Location dependent disclosure risk based decision support framework for persistent authentication in pervasive computing applications. *Computer Networks*, 88:161–177, 2015b.

U. S. Premarathne, I. Khalil, and M. Atiquzzaman. Secure and reliable surveillance over cognitive radio sensor networks in smart grid. *Pervasive and Mobile Computing*, 22:3 – 15, 2015c. Special Issue on Recent Developments in Cognitive Radio Sensor Networks.

U. S. Premarathne, I. Khalil, and M. Atiquzzaman. Trust based reliable transmission strategies for smart home energy management in cognitive radio based smart grid. *Ad Hoc Networks*, 41:15 – 29, 2016. Cognitive Radio Based Smart Grid The Future of the Traditional Electrical Grid.

U. Premaratne, J. Samarabandu, T. Sidhu, B. Beresh, and J. C. Tan. Application of security metrics in auditing computer network security: A case study. In *04th International Conference on Information and Automation for Sustainability*, pages 200–205, Dec 2008.

U. Premaratne, A. Nait-Abdallah, J. Samarabandu, and T. Sidhu. A formal model for masquerade detection software based upon natural mimicry. In *2010 Fifth International Conference on Information and Automation for Sustainability*, pages 14–19. IEEE, 2010a.

U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, and J.-C. Tan. Security analysis and auditing of IEC61850-based automated substations. *IEEE Transactions on Power Delivery*, 25(4):2346–2355, 2010b.

D. Puthal, S. Nepal, R. Ranjan, and J. Chen. A secure big data stream analytics framework for disaster management on the cloud. In *IEEE 18th International Conference on*

High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pages 1218–1225. IEEE, 2016.

C. W. Pyo and M. Hasegawa. Minimum weight routing based on a common link control radio for cognitive wireless ad hoc networks. In *Proceedings of the 2007 international conference on Wireless communications and mobile computing*, pages 399–404. ACM, 2007.

T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao. Towards a trust aware cognitive radio architecture. *ACM SIGMOBILE Mobile Computing and Communication Review*, 13 (2):86 – 95, 2009.

R. C. Qiu, Z. Hu, Z. Chen, N. Guo, R. Ranganathan, S. Hou, and G. Zheng. Cognitive radio network for the smart grid: experimental system architecture, control algorithms, security, and microgrid testbed. *IEEE Transactions on Smart Grid*, 2(4):724–740, 2011.

Z. Quan, S. Cui, and A. H. Sayed. Optimal linear cooperation for spectrum sensing in cognitive radio networks. *IEEE Journal of selected topics in signal processing*, 2(1): 28–40, 2008.

M. Rahimi, J. Ren, C. Liu, A. Vasilakos, and N. Venkatasubramanian. Mobile cloud computing: A survey, state of art and future directions. *Mobile Networks and Applications*, 19(2):133–143, 2014.

R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: the next computing revolution. In *Proceedings of the 47th Design Automation Conference*, pages 731–736. ACM, 2010.

R. Ranchal, B. Bhargava, L. B. Othmane, L. Lilien, A. Kim, M. Kang, and M. Linderman. Protection of identity information in cloud computing without trusted third party. In *Reliable Distributed Systems, 2010 29th IEEE Symposium on*, pages 368–372. IEEE, 2010.

T. Rault, A. Bouabdallah, and Y. Challal. Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks*, 67:104–122, 2014.

M. Rausand and A. Høyland. *System reliability theory: models, statistical methods, and applications*, volume 396. John Wiley & Sons, 2004.

I. Ray and I. Ray. Trust-based access control for secure cloud computing. In *High Performance Cloud Auditing and Applications*, pages 189–213. Springer, 2014.

M. H. Rehmani, A. C. Viana, H. Khalife, and S. Fdida. Surf: A distributed channel selection strategy for data dissemination in multi-hop cognitive radio networks. *Computer Communications*, 36(10):1172–1185, 2013.

H. Reyes, S. Subramaniam, N. Kaabouch, and W. C. Hu. A spectrum sensing technique based on autocorrelation and euclidean distance and its comparison with energy detection for cognitive radio networks. *Computers & Electrical Engineering*, 52:319–327, 2016.

S. Ries. Extending bayesian trust models regarding context-dependence and user friendly representation. In *ACM Symposium on Applied Computing*, SAC '09, pages 1294–1301, 2009. ISBN 978-1-60558-166-8.

T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *16th ACM conference on Computer and communications security*, pages 199–212. ACM, 2009.

S. Roche, E. Propeck-Zimmermann, and B. Mericskay. Geoweb and crisis management: Issues and perspectives of volunteered geographic information. *GeoJournal*, 78(1):21–40, 2013.

M. Rostami, J. B. Wendt, M. Potkonjak, and F. Koushanfar. Quo vadis, puf?: Trends and challenges of emerging physical-disorder based security. In *Proceedings of the Conference on Design, Automation & Test in Europe*, DATE '14, pages 352:1–352:6. European Design and Automation Association, 2014.

R. M. Royall. On finite population sampling theory under certain linear regression models. *Biometrika*, 57(2):377–387, 1970.

U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber. Modeling attacks on physical unclonable functions. In *17th ACM conference on Computer and communications security*, pages 237–249. ACM, 2010.

V. Salmani, S. T. Zargar, and M. Naghibzadeh. A modified maximum urgency first scheduling algorithm for real-time tasks. *Transactions on Engineering, Computing and Technology, ISSN 1305*, 5313:19–23, 2005.

P. Samarati. Protecting respondents identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6):1010–1027, 2001.

U. Sammapun, I. Lee, and O. Sokolsky. Rt-mac: Runtime monitoring and checking of quantitative and probabilistic properties. In *Proceedings. 11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, pages 147–153. IEEE, 2005.

R. V. Sampangi and K. Hawkey. Who are you? it depends (on what you ask me!): Context-dependent dynamic user authentication. In *12th Symposium on Usable Privacy and Security (SOUPS)*, 2016.

O. B. Samuel, M. Z. Khalid, I. Raw, K. Singh, P. Kaur, et al. Highest reliability provides a world class benchmark for permanent downhole monitoring installation and data delivery in malaysia. In *IADC/SPE Asia Pacific Drilling Technology Conference*. Society of Petroleum Engineers, 2014.

J. R. San Cristóbal. *Multi criteria analysis in the renewable energy industry*. Springer Science & Business Media, 2012.

M. Sathiamoorthy, M. Asteris, D. Papailiopoulos, A. G. Dimakis, R. Vadali, S. Chen, and D. Borthakur. Xoring elephants: Novel erasure codes for big data. In *Proceedings of the VLDB Endowment*, volume 6, pages 325–336. VLDB Endowment, 2013.

M. Satyanarayanan. Pervasive computing: Vision and challenges. *IEEE Personal communications*, 8(4):10–17, 2001.

M. Satyanarayanan, G. Lewis, E. Morris, S. Simanta, J. Boleng, and K. Ha. The role of cloudlets in hostile environments. *IEEE Pervasive Computing*, 12(4):40–49, 2013.

E. Scalavino, G. Russello, R. Ball, V. Gowadia, and E. C. Lupu. An opportunistic authority evaluation scheme for data security in crisis management scenarios. In *05th ACM Symposium on Information, Computer and Communications Security*, pages 157–168. ACM, 2010.

A. Scarfo. New security perspectives around byod. In *07th International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA)*, pages 446–451. IEEE, 2012.

S. Schechter. Quantitatively differentiating system security. In *01st Workshop on Economics and Information Security*, pages 16–17. Citeseer, 2002.

S. E. Schechter. Toward econometric models of the security risk from remote attacks. *IEEE Security & Privacy*, 3(1):40–44, 2005.

Y. Selén, H. Tullberg, and J. Kronander. Sensor selection for cooperative spectrum sensing. In *03rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 1–11. IEEE, 2008.

G. Selimis, M. Konijnenburg, M. Ashouei, J. Huisken, H. de Groot, V. van der Leest, G.-J. Schrijen, M. van Hulst, and P. Tuyls. Evaluation of 90nm 6t-sram as physical unclonable function for secure key generation in wireless sensor nodes. In *IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 567–570. IEEE, 2011.

G. Shah, V. C. Gungor, O. B. Akan, et al. A cross-layer qos-aware communication framework in cognitive radio sensor networks for smart grid applications. *IEEE Transactions on Industrial Informatics*, 9(3):1477–1485, 2013.

T. Shah, A. Yavari, K. Mitra, S. Saguna, P. P. Jayaraman, F. A. Rabhi, and R. Ranjan. Remote health care cyber-physical system: quality of service (qos) challenges and opportunities. *IET Cyper-Phys. Syst.: Theory & Appl.*, 1(1):40–48, 2016.

F. Sheikholeslami, M. Nasiri-Kenari, and F. Ashtiani. Optimal probabilistic initial and target channel selection for spectrum handoff in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 14(1):570–584, 2015.

H.-P. Shiang and M. Van der Schaar. Queuing-based dynamic channel selection for heterogeneous multimedia applications over cognitive radio networks. *IEEE Transactions on Multimedia*, 10(5):896–909, 2008.

K. Shilton. Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM*, 52(11):48–53, 2009.

J. Shlens. Notes on kullback-leibler divergence and likelihood. *arXiv preprint arXiv:1404.2000*, 2014.

N. Shlomo. Probabilistic record linkage for disclosure risk assessment. In *Privacy in Statistical Databases*, pages 269–282. Springer, 2014.

S. Singh, M. Woo, and C. S. Raghavendra. Power-aware routing in mobile ad hoc networks. In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pages 181–190. ACM, 1998.

J. So and W. Sung. Group-based multibit cooperative spectrum sensing for cognitive radio networks. *IEEE Transactions on Vehicular Technology*, 65(12):10193–10198, 2016.

A. Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Pérez-Martínez, R. Di Pietro, D. N. Perrea, et al. Smart health: a context-aware health paradigm within smart cities. *IEEE Communications Magazine*, 52(8):74–81, 2014.

Y. Song and J. Xie. Common hopping based proactive spectrum handoff in cognitive radio ad hoc networks. In *Global Telecommunications Conference (GLOBECOM 2010)*, pages 1–5. IEEE, 2010.

Y. Song and J. Xie. Prospect: A proactive spectrum handoff framework for cognitive radio ad hoc networks without common control channel. *IEEE Transactions on Mobile Computing*, 11(7):1127–1139, 2012.

A. Soomro and D. Cavalcanti. Opportunities and challenges in using wpan and wlan technologies in medical environments [accepted from open call]. *IEEE Communications Magazine*, 45(2):114–122, 2007.

E. Spanò, S. Di Pascoli, and G. Iannaccone. Low-power wearable ecg monitoring system for multiple-patient remote monitoring. *IEEE Sensors Journal*, 16(13):5452–5462, 2016.

A. C. Squicciarini, A. Trombetta, E. Bertino, and S. Braghin. Identity-based long running negotiations. In *04th ACM Workshop on Digital Identity Management*, pages 97–106. ACM, 2008.

A. C. Squicciarini, E. Bertino, A. Trombetta, and S. Braghin. A flexible approach to multisession trust negotiations. *IEEE Transactions on Dependable and Secure Computing*, 9(1):16–29, 2012.

W. Stadler. Fundamentals of multicriteria optimization. In *Multicriteria Optimization in Engineering and in the Sciences*, pages 1–25. Springer, 1988.

W. Stallings. *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

G. Stevens. Data security breach notification laws. http://fas.org/sgp/crs/misc/R42475.pdf, 2012.

C. Sun, W. Zhang, and K. Ben. Cluster-based cooperative spectrum sensing in cognitive radio systems. In *IEEE International Conference on Communications (ICC)*, pages 2511–2515. IEEE, 2007.

P. Sun, Q. Shen, Y. Chen, Z. Wu, C. Zhang, A. Ruan, and L. Gu. Poster: Lbms: load balancing based on multilateral security in cloud. In *18th ACM Conference on Computer and Communications security*, pages 861–864. ACM, 2011.

S. Sundareswaran and A. C. Squcciarini. Detecting malicious co-resident virtual machines indulging in load-based attacks. In *Information and Communications Security*, pages 113–124. Springer, 2013.

N. K. Suryadevara, S. C. Mukhopadhyay, S. D. T. Kelly, and S. P. S. Gill. Wsn-based smart sensors and actuator for power management in intelligent buildings. *IEEE/ASME Transactions On Mechatronics*, 20(2):564–571, 2015.

A. Tadaion. Notice of proposed rule making: unlicensed operation in the tv broadcast bands. *ET Docket*, (04-186), 2004.

C. Talcott. Cyber-physical systems and events. *Software-Intensive Systems and New Computing Paradigms*, pages 101–115, 2008.

Z. Tari, X. Yi, U. Premarathne, P. Bertok, and I. Khalil. Security and privacy in cloud computing: Vision, trends, and challenges. *IEEE Cloud Computing*, 2(2):30–38, Mar 2015.

D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem. A platform for secure monitoring and sharing of generic health data in the cloud. *Future Generation Computer Systems*, 35:102–113, 2014.

K. Thirunarayan, P. Anantharam, C. Henson, and A. Sheth. Comparative trust management with applications: Bayesian approaches emphasis. *Future Generation Computer Systems*, 31:182–199, 2014.

I. Thomas, M. Menzel, and C. Meinel. Using quantified trust levels to describe authentication requirements in federated identity management. In *ACM Workshop on Secure Web services*, pages 71–80. ACM, 2008.

G. Tonti, J. M. Bradshaw, R. Jeffers, R. Montanari, N. Suri, and A. Uszok. Semantic web languages for policy representation and reasoning: A comparison of kaos, rei, and ponder. In *The Semantic Web (ISWC)*, pages 419–437. Springer, 2003.

V. Torra. Towards the re-identification of individuals in data files with non-common variables. In *14th European Conference on Artificial Intelligence (ECAI)*, pages 326–332, 2000.

V. Torra, J. M. Abowd, and J. Domingo-Ferrer. Using mahalanobis distance-based record linkage for disclosure risk assessment. In *Privacy in Statistical Databases*, pages 233–242. Springer, 2006.

F. F. Townsend et al. The federal response to hurricane Katrina: Lessons learned. *Washington, DC: The White House*, 2006.

E. Z. Tragos, S. Zeadally, A. G. Fragkiadakis, and V. A. Siris. Spectrum assignment in cognitive radio networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 15(3):1108–1135, 2013.

T. M. Truta and B. Vinay. Privacy protection: p-sensitive k-anonymity property. In *22nd International Conference on Data Engineering Workshops*, pages 94–94. IEEE, 2006.

M. Tupper and A. N. Zincir-Heywood. Vea-bility security metric: A network security analysis tool. In *03rd International Conference on Availability, Reliability and Security (ARES)*, pages 950–957. IEEE, 2008.

K. Tutuncuoglu and A. Yener. Optimum transmission policies for battery limited energy harvesting nodes. *IEEE Transactions on Wireless Communications*, 11(3):1180–1189, 2012.

A. Ullah, J. Li, A. Hussain, and Y. Shen. Genetic optimization of fuzzy membership functions for cloud resource provisioning. In *IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1–8. IEEE, 2016.

S. Voigt, T. Kemper, T. Riedlinger, R. Kiefl, K. Scholte, and H. Mehl. Satellite image analysis for disaster and crisis-management support. *IEEE transactions on Geoscience and Remote Sensing*, 45(6):1520–1528, 2007.

A. Vosoughi, J. R. Cavallaro, and A. Marshall. A cooperative spectrum sensing scheme for cognitive radio ad hoc networks based on gossip and trust. In *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 1175–1179. IEEE, 2014.

A. Wald. On cumulative sums of random variables. *The Annals of Mathematical Statistics*, 15(3):283–296, 1944.

C.-W. Wang, L.-C. Wang, and F. Adachi. Modeling and analysis for reactive-decision spectrum handoff in cognitive radio networks. In *Global Telecommunications Conference (GLOBECOM 2010)*, pages 1–6. IEEE, 2010.

H. Wang, Y. Qian, and H. Sharif. Multimedia communications over cognitive radio networks for smart grid applications. *IEEE Wireless Communications*, 20(4), 2013.

J. Wang, S. Feng, Q. Wu, X. Zheng, Y. Xu, and G. Ding. A robust cooperative spectrum sensing scheme based on dempster-shafer theory and trustworthiness degree calculation in cognitive radio networks. *EURASIP Journal on Advances in Signal Processing*, 2014 (1):35, 2014a.

J. Wang, R. Chen, J. J. Tsai, and D.-C. Wang. Trust-based cooperative spectrum sensing against ssdf attacks in distributed cognitive radio networks. In *International Workshop Technical Committee on Communications Quality and Reliability (CQR 2016)*, pages 1–6. IEEE, 2016a.

K. Wang, S. Jiang, X. Ma, Z. Wu, H. Shao, W. Zhang, and C. Cui. Numerical simulation and application study on a remote emergency rescue system during a belt fire in coal mines. *Natural Hazards*, 84(2):1463–1485, 2016b.

L.-C. Wang, C.-W. Wang, and G. Feng. A queueing-theoretical framework for qos-enhanced spectrum management in cognitive radio networks. *IEEE Wireless Communications*, 18(6):18–26, 2011.

L.-C. Wang, C.-W. Wang, and C.-J. Chang. Modeling and analysis for spectrum handoffs in cognitive radio networks. *IEEE Transactions on Mobile Computing,*, 11(9):1499–1513, 2012.

N. Wang, N. Zhang, and M. Wang. Wireless sensors in agriculture and food industryrecent development and future perspective. *Computers and electronics in agriculture*, 50(1): 1–14, 2006.

Q. Wang, H. Jin, and N. Li. Usable access control in collaborative environments: Authorization based on people-tagging. In *Computer Security (ESORICS)*, pages 268–284. Springer, 2009.

X. Wang and M. Tehranipoor. Novel physical unclonable function with process and environmental variations. In *Conference on Design, Automation and Test in Europe*, pages 1065–1070. European Design and Automation Association, 2010.

Y. Wang, J. Wei, and K. Vangury. Bring your own device security issues and challenges. In *11th Consumer Communications and Networking Conference (CCNC)*, pages 80–85. IEEE, 2014b.

Y. Wang, W. Lin, R. Sun, and Y. Huo. Optimization of relay selection and ergodic capacity in cognitive radio sensor networks with wireless energy harvesting. *Pervasive and Mobile Computing*, 22:33–45, 2015.

E. U. Weber. Risk attitude and preference. *Wiley Interdisciplinary Reviews: Cognitive Science*, 1(1):79–88, 2010.

E. U. Weber and R. A. Milliman. Perceived risk attitudes: Relating risk perception to risky choice. *Management science*, 43(2):123–144, 1997.

D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde. Protecting smart grid automation systems against cyberattacks. *IEEE Transactions on Smart Grid*, 2(4):782–795, 2011.

J. Wei and X. Zhang. Energy-efficient distributed spectrum sensing for wireless cognitive radio networks. In *IEEE Conference on Computer Communications Workshops (INFOCOM)*, pages 1–6. IEEE, 2010.

S. Wei and M. Potkonjak. Wireless security techniques for coordinated manufacturing and on-line hardware trojan detection. In *05th ACM conference on Security and Privacy in Wireless and Mobile Networks*, pages 161–172. ACM, 2012.

M. Weichold, M. Hamdi, M. Z. Shakir, M. Abdallah, G. K. Karagiannidis, and M. Ismail. *Cognitive Radio Oriented Wireless Networks: 10th International Conference, CROWNCOM 2015, Doha, Qatar, April 21-23, 2015, Revised Selected Papers*, volume 156. Springer, 2015.

J. Werner, C. M. Westphall, and C. B. Westphall. Cloud identity management: A survey on privacy strategies. *Computer Networks*, 122:29–42, 2017.

L. Willenborg and T. De Waal. *Elements of statistical disclosure control*, volume 155. Springer Science & Business Media, 2012.

A. Wool. A quantitative study of firewall configuration errors. *Computer*, 37(6):62–67, 2004.

D. Wu, J. He, H. Wang, C. Wang, and R. Wang. A hierarchical packet forwarding mechanism for energy harvesting wireless sensor networks. *IEEE Communications Magazine*, 53(8):92–98, 2015.

Y. Wu, F. Hu, S. Kumar, Y. Zhu, A. Talari, N. Rahnavard, and J. D. Matyjas. A learning-based qoe-driven spectrum handoff scheme for multimedia transmissions over cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 32(11):2134–2148, 2014.

Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren. A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. *IEEE Transactions on Information Forensics and Security*, 11(11):2594–2608, 2016.

B. Xu, L. Da Xu, H. Cai, C. Xie, J. Hu, and F. Bu. Ubiquitous data accessing method in iot-based information system for emergency medical services. *IEEE Transactions on Industrial Informatics*, 10(2):1578–1586, 2014.

D. Xu and X. Liu. Opportunistic spectrum access in cognitive radio networks: when to turn off the spectrum sensors. In *04th Annual International Conference on Wireless Internet*, page 13. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

L. Yan, C. Rong, and G. Zhao. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In *Cloud Computing*, pages 167–177. Springer, 2009.

K. Yang, K. Zheng, Y. Guo, and D. Wei. Puf-based node mutual authentication scheme for delay tolerant mobile sensor network. In *07th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, pages 1–4. IEEE, 2011.

F. Ye, G. Zhong, J. Cheng, S. Lu, and L. Zhang. Peas: A robust energy conserving protocol for long-lived sensor networks. In *23rd international conference on Distributed computing systems*, pages 28–37. IEEE, 2003.

S. Yin, D. Chen, Q. Zhang, M. Liu, and S. Li. Mining spectrum usage data: a large-scale spectrum measurement study. *IEEE Transactions on Mobile Computing*, 11(6): 1033–1046, 2012.

H. L. Younes, M. Kwiatkowska, G. Norman, and D. Parker. Numerical vs. statistical probabilistic model checking. *International Journal on Software Tools for Technology Transfer*, 8(3):216–228, 2006.

M. Younis, M. Youssef, and K. Arisha. Energy-aware routing in cluster-based sensor networks. In *10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 2002. MASCOTS 2002.*, pages 129–136. IEEE, 2002.

M. Youssef, M. Ibrahim, M. A. Latif, L. Chen, and A. V. Vasilakos. Routing metrics of cognitive radio networks: A survey. *IEEE Communications Surveys and Tutorials*, 16 (1):92–109, 2014.

P.-L. Yu and G. Leitmann. Compromise solutions, domination structures, and salukvadze's solution. *Journal of Optimization Theory and Applications*, 13(3):362–378, 1974.

R. Yu, Y. Zhang, L. Yi, S. Xie, L. Song, and M. Guizani. Secondary users cooperation in cognitive radio networks: balancing sensing accuracy and efficiency. *IEEE Wireless Communications*, 19(2):30–37, 2012.

S. Yu, C. Wang, K. Ren, and W. Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing. In *IEEE International Conference on Computer Communications (INFOCOM)*, pages 1–9. Ieee, 2010.

T. Yu and M. Winslett. Policy migration for sensitive credentials in trust negotiation. In *Proceedings of the 2003 ACM workshop on Privacy in the Electronic Society*, pages 9–20. ACM, 2003.

T. Yu, M. Winslett, and K. E. Seamons. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. *ACM Transactions on Information and System Security (TISSEC)*, 6(1):1–42, 2003.

T. Yücek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Communications Surveys & Tutorials*, 11(1):116–130, 2009.

G. Zhang and M. Parashar. Context-aware dynamic access control for pervasive applications. In *Communication Networks and Distributed Systems Modeling and Simulation Conference*, pages 21–30, 2004.

L. Zhang, T. Song, M. Wu, J. Guo, D. Sun, and B. Gu. Modeling for spectrum handoff based on secondary users with different priorities in cognitive radio networks. In *International Conference on Wireless Communications & Signal Processing (WCSP)*, pages 1–6. IEEE, 2012.

W. Zhang and C. K. Yeo. Sequential sensing based spectrum handoff in cognitive radio networks with multiple users. *Computer Networks*, 58:87–98, 2014.

W. Zhang, R. K. Mallik, and K. B. Letaief. Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 8(12):5761–5766, 2009.

Y. Zhang, A. Juels, A. Oprea, and M. K. Reiter. Homealone: Co-residency detection in the cloud via side-channel analysis. In *IEEE Symposium on Security and Privacy*, pages 313–328, 2011.

Y. Zhang, T. Jiang, L. Zhang, D. Qu, and W. Peng. Analysis on the transmission delay of priority-based secondary users in cognitive radio networks. In *International Conference on Wireless Communications Signal Processing (WCSP)*, pages 1–6, Oct 2013a.

Y. Zhang, F. Zhang, Y. Shakhsheer, J. D. Silver, A. Klinefelter, M. Nagaraju, J. Boley, J. Pandey, A. Shrivastava, E. J. Carlson, et al. A batteryless 19 w mics/ism-band energy harvesting body sensor node soc for exg applications. *IEEE Journal of Solid-State Circuits*, 48(1):199–213, 2013b.

H. Zhao and X. Li. Vectortrust: trust vector aggregation scheme for trust management in peer-to-peer networks. *The Journal of Supercomputing*, 64(3):805–829, 2013.

D. Zissis and D. Lekkas. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3):583–592, 2012.

B. Zwattendorfer, K. Stranacher, and A. Tauber. Towards a federated identity as a service model. In *Technology-Enabled Innovation for Democracy, Government and Governance*, pages 43–57. Springer, 2013.