View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by espace@Curtin

© 2011 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

A Combinational Approach for Trust Establishment in Cognitive Radio Networks

Sazia Parvin, Song Han, Farookh Khadeer Hussain, Biming Tian
Digital Ecosystems & Business Intelligence Institute
Curtin University of Technology, Australia
Perth, Australia
{sazia.parvin, biming.tian}@postgrad.curtin.edu.au, {Song. Han; Farookh.Hussain} @cbs.curtin.edu.au

***Abstract*—Cognitive Radio is considered as a promising and demanding technology to examine whether a particular radio spectrum band is currently in use or not and to switch into the temporarily unoccupied spectrum band in order to improve the usage of the radio electromagnetic spectrum without creating interference to the transmissions of other users. Because of the dynamic properties of CRNs, the issue of supporting secure communication in CRNs becomes more critical than that of other conventional wireless networks. In this paper, we propose a combination of certificate-based trust with a behavior-based trust which will benefit both by representing the trust as certificates in the the predeployment trust relation and by providing a continuous behaviour-based evalution of trust.**

Keywords- Trust, primary user, secondary user, security, cognitive radio networks, radio.

I. INTRODUCTION

Due to the increasing demand for new wireless services and applications, Cognitive Radio (CR) has offered a promising concept for improving the consumption of limited radio spectrum resources for future wireless communications and mobile computing [13]. The primary objective of Cognitive Radio Networks is to scan the spectrum and identity free channels which will be used for opportunistic transmission. Sometimes, several frequency bands are not used according to their maximum level. These under-utilized areas are known as spectrum holes or white spaces [1]. So, CRs offer a solution for the scarcity of spectrum by reusing the under-utilized spectrum. National regulatory bodies like the Federal Communications Commission (FCC) assign spectrum for particular types of services that are then licensed to bidders for a fee [2]. CR, pioneered by Mitola [3] from software defined radio (SDR), was mainly considered to make a better utilization of spectrum. CR, on the other hand, takes place above the SDR and is the "intelligence" that lets an SDR determine which mode of operation and parameters to use [23]. We can obtain an overview of CR functionalities from Haykins's definition of cognitive radio [4]: "Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understandings-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit power, carries-frequency, and modulation strategy) in real time, with two primary objectives in mind: highly reliable communication whenever and wherever needed, efficient utilization of the radio spectrum". CR has two main properties: Artificial Intelligence (AI) and Dynamic Spectrum Access (DNS) [5]. AI involves reasoning and learning. This gives CR its 'intelligent' characteristics and allows it to learn about its changing environment. DNS refers to the processes involved in getting a CR to detect and occupy a vacant spectrum. It involves spectrum sensing, spectrum management, spectrum mobility and spectrum sharing. Generally, there are two types of users in CR: the primary user (PU) is a licensed user of a particular radio frequency band [6]; and the secondary user (SU) is an unlicensed user who operates in a cognitive way without making harmful interference to the primary user [6]. Since cognitive radios can adapt to their radio environment and has ability to change how they communicate, so it is critical that they choose optimal and secure communications. The unique characteristics of CRNs make security more challenging [13]. Still, there are some crucial issues which have not been investigated in the area of security for cognitive radio networks. When a CR node initially tries to form a CRN, or tries to connect a node which is intended to join an existing CRN, it is practically quite impossible to implement conventional security functions as CRNs have resource constraints such as power and memory [24]. The common public key infrastructure (PKI) scheme which achieves secure routing and other purposes in typical ad-hoc networks is not enough to guarantee the security for CRNs under limited communication and computation resources [24]. Even the various encryption techniques such as public key encryption (RSA, Elliptic, SHA) and private key encryption (DES, Triple DES, AES) algorithms can be used in CRNs to provide a form of secure communication [21]. All of these encryption algorithms need to make sure that the key that is used at the transmitter side should be provided by the receiver for correct informational retrieval thereby ensuring the security and also preventing any malicious users from taking control of the system and blocking other secondary users' access [21]. Therefore, CRNs require a trusted mechanism, while authentication is a component of trust along with other technical or non-technical factors. To ensure the smooth and normal operation of CRNs, trust forms the foundation of the security platform of CRNs with a view to support ubiquitous and mobile computing. However, trust for CRNs is quite different from that of other wireless scenarios and in other areas of computing trust. Trust is critical in CRNs' operation and is

beyond security design since security usually needs communication overhead advance [9]. So in this paper, we propose a combinational approach to establish trust in cognitive radio networks (CRNs) in order to ensure security in communication.

This paper is organized as follows: In Section 2, related works is reviewed. In Section 3, we describe the basics of trust. In Section 4, we describe our proposed scheme which combines a certificate-based and behavior-based trust scheme. We conclude the paper in Section 5 including remarks on future directions.

II. RELATED WORKS

It is mentioned that trust has been widely mentioned in the existing literatures in relation to trusted computing and web computing, ad hoc networks and even social science [8]. To ensure the smooth operation of CRNs to support ubiquitous and mobile computing, establishing trust for CRNs is an open and challenging issue. However, trust for CRNs is completely different from trust in these other aspects and scenarios. Trust is critical in CRNs operation and beyond security design, as security usually needs communication overhead in advance [9]. The authors in [9] describe the trust in CRN as an essential component of CRNs.

The authors in [10] proposed a Markov chain-based trust model has been proposed for analyzing trust value in distributed multicasting mobile ad hoc networks. They also proposed the approach for selecting the Certificate Authority (CA) and Backup CA (BCA) [10]. Essential and important considerations for developing a good trust management system for Wireless Sensor Networks (WSNs) have been proposed in [18]. The impact of trust model in CRNs is discussed briefly in [11]. Parvin et al. [22] proposed trust-based security for cognitive radio networks. They presented a trust-based matrix for calculating trust value, but they did not show the evaluation process in detail. The authors in [12] integrated trust and reputation for the threat mitigation of Spectrum Sensing Data Falsification (SSDF) attack on CRNs. However, they did not propose any trust modeling for CRNs. The authors suggested potential ways for applying trust modeling to CRNs including identity management, the trust building process and possible mechanisms for disseminating the trust information [11]. Furthermore, no experimental results were established to support these discussions. A trust-aware model was proposed for spectrum sensing in CRNs but the authors fail to evaluate the system [13]. A Trust Value Updated Model (TVUM) is proposed in layered and grouped ad-hoc network for ensuring the authentication [14]. In this paper, we propose a combinational trust-establishment approach for secure communication in CRNs.

III. TRUST IN COGNITIVE RADIO NETWWORKS

Some nodes in Cognitive Radio Networks become compromised and cause harm to the open and shared wireless networks. Current research is concerned with detecting these malicious harmful nodes and finding a means to exclude them from the network. In this paper, our intension is to establish the effectiveness of trust in this regard. In a trust-based CRNs model, the main objectives of trust are to manage the CR nodes in a dynamic manner and the cognitive radio nodes' activity is monitored and evaluated effectively in a distributed manner. Based on the trust evaluation model, malicious nodes are detected and listed in a blacklist so that they cannot take part further in any communication within the network community. Therefore, trust-establishment for evaluating trust is beneficial for secure communication in CRNs.

A. Definition of Trust

According to [15], trust is a mutual relationship between two parties so that one party can believe, expect, and accept that the other trusted party will act or intend to act accordingly. Based on our CRNs working principles, we express trust as a representation of the degree to which a cognitive radio node would communicate with other cognitive radio nodes in a trustworthy, secure, or reliable way. There are various ways to measure the trust value and we represent the trust by symbol T. In our cognitive radio network model, when a secondary user represents trustworthiness enough for a primary user and satisfies the basic trust requirements, only then the secondary user can obtain access to the free spectrum of the primary user and participate in the communication initiated by that secondary user.

B. Trust Establishment in CRNs

There are two different ways to establish trust in CRNs.

- Certificate –based Trust Establishment

Certificate-based trust establishment is a traditional and the most widely used approach. A public key infrastructure model is used to set up the Certificate Authority (CA) in this framework. Three standard approaches have been proposed in [15] for establishing certificate-based trust. These three approaches are different from each other based on the architecture. Among these three approaches, two are based on hierarchical architecture and one is on distributed architecture. In hierarchical-based approach, the trusted third party is responsible for the evaluation of trust by using signed certificates. A self-organized public key management scheme is used in the second approach, where certificate chains are used to evaluate trust value. In the third approach, secret key sharing mechanisms play an important role to circulate the trust to an aggregation of nodes which is able to provide continuous services to CA.

- Behavior –based Trust Establishment

In the behavior-based trust model, trust is considered as the degree of positive cooperation and behaviors between surrounding CR nodes in the CRNs. Trust is evaluated in both independent and cooperative manner. In an independent manner, trust is evaluated by every CR node using local observations and statistical data that is integrated by continuous monitoring the traffic of cognitive radio network. However, in a cooperative manner, trust is evaluated by sharing recommendations with neighboring nodes and distributing reputation among neighboring nodes. The main purpose of the behavior-based trust model is to detect the

malicious CR nodes, isolate them in order to protect resources of the network, by assigning a low trust value and sending a recommendation to other nodes not to establish any further communication with the malicious CR nodes .

When trust is evaluated independently, it is called 'direct trust'. In 'direct trust', the evaluation is based on the direct communication and experience that the trustor CR node has on the trustee CR node. Mechanisms of collecting evidences usually take place under the application layer, in order to measure the evaluation of routing behaviors and information of integrity [16]. For example, the radio in every CR node always needs to be activated, while the trust values of all neighboring nodes in the network are required to be stored and updated continuously whenever interactions take place in the network.

'Indirect' trust is measured according to the recommendations from other nodes about the target node. The derivation procedure of indirect trust needs to weight the recommendations from other nodes depending on how much trusted they are [19, 20] or providing secret and confidential information with the recommendations [20]. The result of the exchange of recommendations for evaluating indirect trust is then spread through the whole cognitive radio network. Selfishness behavior and unwillingness attitude are the major drawbacks of the 'indirect trust' method to spread the information regarding reputation throughout the whole network.

The functions and notations [16] that are involved in calculating the trust value for the trustor CR node (i) to the trustee CR node (j) in behavior-based trust frameworks is as follows:

- A function $T_D(i, j)$ for evaluating the direct trust value experienced from past interactions and based on network-based traffic monitoring metrics [16].
- A function $T_{ID}(i, j)$ for evaluating the indirect trust value depending on recommendations from other neighboring CR nodes about the target node.
- A function $T(i, j)$ for evaluating the final target trust value by using both direct and indirect trust. This final trust ($T(i, j)$) value is compared with the trust threshold for various purpose in the network.

C. Trust Relationship

Trust is defined as a mutual relationship between two entities for a specific action. Trust is defined by 'T'. The notation indicates the trust relationship between CR node A and CR node B. If one CR node trusts another CR node for a specific purpose, a reliable trust relationship is established between these two communicating nodes. Let us assume that for two CR nodes where A is the primary user and B is the secondary user, the trust value of A to B is T_{AB}. If B sends a request to A to use its free spectrum, A checks whether it is good enough to assign the free spectrum to B. If A does not have any past trust relationship with B, then A will evaluate the trust value using reference or recommendations which is called 'Indirect Trust'. Whenever one node communicates, its activity is monitored and if it communicates successfully, its trust value is increased.

D. Trust Factors in CRNs

In this section, we describe how different trust factors influence the trust management system in CRNs.

We have described a set of different trust factors as follows:

1) Trust and Reputation: Trust and reputation should be calculated separately in the trust management system in CRNs. These values could be considered as input for determining the trust values. Sometimes trust is not calculated directly from the behavior of one node; then, it is better to consider the previous reputation in order to determine the trustworthiness of a node. For example, a malicious node could suddenly become good. So it is not a wise decision to trust that malicious node, based on its previous reputation.
2) Trust and Base Station: The base station should participate in the trust management system [18] in CRNs. Both base stations (primary user base station, secondary user base station) use the information produced by the corresponding CR members in CRNs to observe, analyze the behavior of the CR nodes. The base station stores the reputation value of the corresponding node and makes a global trust decision using these values. The correspondence between the base station and the CR nodes can be made by using secure communication mechanisms such as public key cryptography.
3) Direct Information: The events performed by a certain CR node can be used as input for the trust management system in CRNs. Suppose node X has direct communication with node Y. So node X can measure trust value of node Y depending on the various events that it performed during their communication. Direct information should be taken into consideration during the development of the trust management system in CRNs. Trust information from different sources is more reliable when creating a robust trust system.
4) Indirect Information: Reputation-based information about all other nodes should be distributed among all the CRNs. So, one node can easily obtain information about other node which is not directly linked to that node. For developing of trust management system, we should consider all indirect information carefully as failure to use indirect information may influence the result in decisions which are inconsistent with the CRNs.
5) Initial values: At the initial stage, the trust management system must set the initial values of trust and reputation of the network before the

deployment. At the initial stage of the deployment, all nodes must have a good reputation and be equally trusted [18]. At the very beginning of the deployment, any malicious adversary had neither the time nor the chance to influence or subvert a node [18]. New nodes that appear after the deployment should not be trusted as they might be adversarial or malicious.

6) Degree of trust: For a better trust management system, the degree of trust during the calculation of trust and reputation of a CR node should be taken into consideration. The reputation of a node depends on its past behavior and the actions performed by the node.
7) Updating the trust value: The trust management system must be updated in a timely manner. It is recommended that the trust value be checked at pre-determined time intervals and that the previous trust management system is updated if necessary.
8) Risk and importance : According to [18], there are two factors that influence the calculation of the trust values for a CR node, one is the risk of the interaction between the trustor and the trustee and the other is the importance of the reputation value in that specific interaction. Risk and importance also influence the selection of the trust threshold value for the CRNs.

IV. Combinational Approach for Trust Establishment in CRNs.

In this section, we propose a combinational approach for establishing trust in CRNs which integrates the features of both certificate-based and behavior-based methods of establishing trust. The main objective and motivation of this approach is to reap the benefits of both methods. The pre-deployment trust relationship is represented by certificate-based trust establishment, and behavior-based trust is established throughout the whole network during the communication.

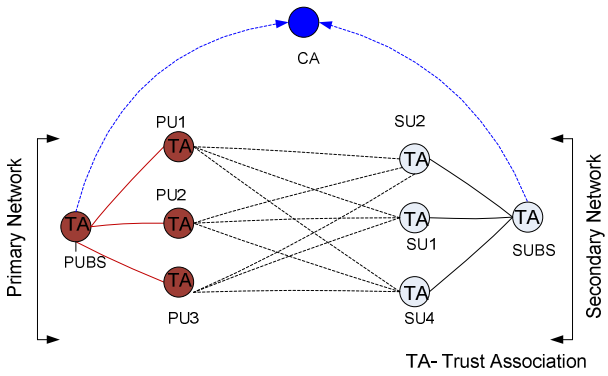

Fig 1: System model of Proposed Scheme

In our proposed model, we want to show how trust establishment affects the model.

The trust associations (TA) between any CR node i and any node j in both networks work are as follows:

1. Trust associations are stored in each CR node locally before deployment.
2. A hierarchical trust relationship is established in the network so that CR node j is considered trusted by node i . For example, if node j has a valid certificate, node i can verify its trust value based on the public key which is stored on trust managing authority (CA). Trust associations in the network can be measured between nodes that are associated with common trust managing authorities (CA) who is responsible to issue the certificates for a particular deployment.
3. A cooperative process is established so that node i asks for recommendations for node j from nodes with which node i has a trust association.

Certificate-based trust establishment:
In our model, the primary user (PU) and secondary user (SU) are deployed in one geographical area. PUs are connected to PUBS (Primary User Base Station) and SUs are connected to SUBS (Secondary User Base Station). Both PUBS and SUBS are connected to the CA (Certificate Authority). In network security, the third party is called the Certificate Authority (CA) who always achieves secure authentication [10]. So the SUs and PUs are connected to CA via SUBS and PUBS respectively. Whenever one SU searches the PU's free available spectrum, the PU is connected to the CA to see the trust value of the requested secondary user. The CA provides the trust-certificates to the Primary user about the requested secondary user.

Behavior-based trust:
When the PU wants to communicate with the SU, it searches the trust value of SU after receiving certificates from CA. If this SU has had previous interaction with this PU, the PU will see the trust association table and check the trust value of SU for previous interactions. This is called 'direct trust' ($T_D(i,j)$).
If the PU does not have any previous communication with the SU, then it will use recommendations from other nodes about the SU. This is called 'Indirect trust' ($T_{ID}(i,j)$). If more than one neighboring node sends recommendations to the PU about SU. Then PU will obtain an average of these recommendations and get at a trust value.
The PU will calculate the final behavioral trust by integrating these two trust values in order to set up a communication link with the requesting node.

$$T(i,j) = T_D + T_{ID}$$

The system will define a trust threshold ($T_{Threshold}$) depending on the system parameter. After calculating the

final trust, this value $T(i,j)$ is compared with the trust threshold value.

If $T(i,j) > T_{Threshold}$, then the requested service is provided to the requesting user.

If $T(i,j) < T_{Threshold}$, then the requested service is discarded.

The whole working process can be represented by the following process:

In the first phase we want to show the interaction between sender and receiver. At first the sender sends one request to the receiver for the desired service.

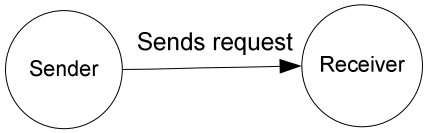

Fig 2: Communication initiates from Sender to Receiver

In this flowchart, we show how both certificate-based and behavior-based trust is established in CRNs.

According to the system model, the working steps of this flowchart are as follows:

1. One secondary user will send request to primary user to use its free spectrum after sensing algorithm applied.
2. The primary user will receive the request from the secondary user and it will check the secondary user's certificate from the CA for security purposes. If the CA does not send any valid certificate for this requesting secondary user, then the primary user will send this information to the base station. Then base station will detect whether it is a malicious node or a hacker.
3. After checking the certificate, the primary user will check whether or not it has had any previous interaction the requesting secondary user. If it has any previous interaction, then it will calculate the trust value based on the previous event that the secondary user performed. Trust from this process is called 'Direct Trust'.
4. If the primary user has not had any previous interaction with the secondary user, then it will collect the recommendations from its neighboring nodes about the requesting secondary user. The primary user will accumulate the recommendations and calculate the trust value. Trust achieved in this way is called 'Indirect Trust'.

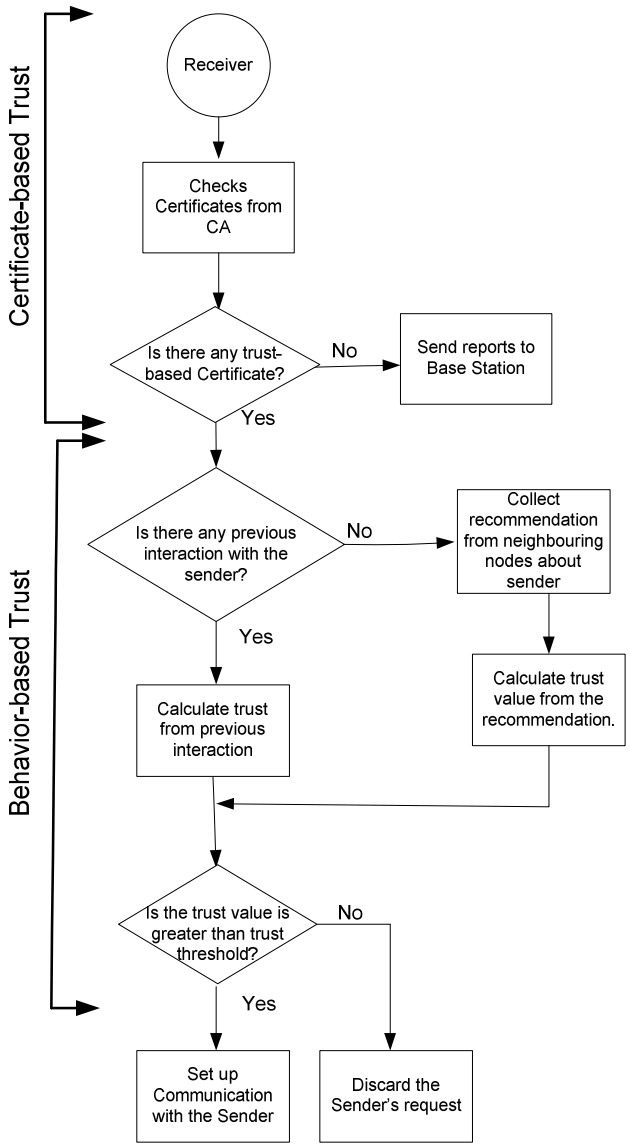

Fig 3: Trust-based working process of Receiver

5. The primary user will calculate the final trust. This trust value is compared with the trust threshold defined by the system based on the system parameters. If the final trust is greater than the trust threshold, the requesting secondary user will obtain its requested service.
6. If the final trust is less than the trust threshold, then the primary user will discard the request.

V. CONCLUSION

This paper is concerned with securing CRNs by establishing both behaviour-based and certificate-based trust in CRNs. Cognitive Radio Networks introduce various types of security attacks to wireless networks comparaed to wired

networks and make the security models and approaches very crucial. Because of the dynamic characteristics of CRNs, a member of CRNs may join or leave the network at any time. So it is more imporatnt to ensure the security of CRNs than that of other conventional wireless networks. In this paper, we propose a combination of certificate-based trust with a behavior-based trust which will benefit both by representing trust as certificates in predeployment trust relationships and by providing a continuous behaviour-based evalution of trust. In our future work, we will focus on the detailed implementation of the proposed scheme in CRNs.

REFERENCES

[1] C. Zenon., et al., *Security threats in Cognitive Radio applications*, in *Intelligent Engineering Systems (INES), 2010 14th International Conference on*. 2010. p. 209-214.

[2] O. Leon, J.H. Serrano, and M.Soriano, *Securing Cognitive Radio Networks.* International Journal of Communication Systems, 2010. **23**(5): p. 633-652..

[3] J. Mitola, *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. PhD thesis,*, in *Royal Institute of Technology (KTH)*. 2000.

[4] S.Haykin, *Cognitive radio: brain-empowered wireless communications* IEEE Journal on Selected Areas in Communications, 2005. **23**(2): p. 201-220.

[5] Y. Zhang, G. Xu, and X. Geng, *Security Threats in Cognitive Radio Networks*, in *Conference on High Performance Computing and Communications*. 2008.

[6] C.N. Mathur, and K.P. Subbalakshmi. *Digital Signatures for Centralized DSA Networks*. in *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*. 2007..

[7] X. Zhang, C.L., *The security in cognitive radio networks: a survey*, in *International Conference On Communications And Mobile Computing* 2009, ACM: Leipzig, Germany p. 309-313.

[8] P. Naldurg, and R.H. Campbell. *Dynamic Access Control: Preserving Safety and Trust in Network Defense Operations*. in *Proceedings of the Eighth ACM Symposium in Access Control Models and Technologies (ACM SACMAT 2003)*. 2003

[9] K.-C. Chen , Y.-J.P., N. Prasad ,Y.-C. Liang ,S. Sun and *Cognitive radio network architecture: part II -- trusted network layer structure*, in *Conference On Ubiquitous Information Management And Communication* 2008, ACM: Suwon, Korea p. 120-124

[10] Ben-Jye, C., et al. *Markov Chain-Based Trust Model for Analyzing Trust Value in Distributed Multicasting Mobile Ad Hoc Networks*. in *Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE*. 2008.

[11] T.C.Clancy, N.G., *Security in Cognitive Radio Networks: Threats and Mitigation*, in *Cognitive Radio Oriented Wireless Networks and Communications, 2008.* . 2008. p. 1-8

[12] R.Chen, J.-M.P., Y. T. Hou,J. H. Reed, *Toward secure distributed spectrum sensing in cognitive radio networks*, in *IEEE Communications Magazine Special Issue on Cognitive Radio Communications*. 2008. p. 50-55

[13] S., Parvin, et al. *Towards Trust Establishment for Spectrum Selection in Cognitive Radio Networks*. in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*. 2010

[14] Y.-t. Yang, et al. *A Novel Authentication Scheme Based on Trust-value Updated Model in Adhoc Network*. in *Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International*. 2007

[15] D.H. McKnight, N.L. Chervany, The Meanings of Trust, Technical Report, University of Minnesota, 1996.

[16] E. Aivaloglou, S. Gritzalis, and C. Skianis, *"Trust establishment in sensor networks: behaviour-based, certificate-based and a combinational approach",* International Journal of System of Systems Engineering 2008. **Volume 1**: p. 128-148.

[17] A. Boukerche, and Y. Ren, "*A trust-based security system for ubiquitous and pervasive computing environments"*. Computer Communications, 2008. 31(18): p. 4343-4351.

[18] J. Lopez, et al., *Trust management systems for wireless sensor networks: Best practices.* Computer Communications, 2010. **33**(9): p. 1086-1093.

[19] S. Ganeriwal and M.B. Srivastava, '*Reputation-based framework for high integrity sensor networks'*, Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN'04), ACM Press, pp.66–77

[20] G. Theodorakopoulos, and J.S. Baras, '*Trust evaluation in ad-hoc networks*', Workshop on Wireless Security, pp.1–10.

[21] S. Sanyal, R. Bhadauria and C. Ghosh, "*Secure Communication in Cognitive Radio Networks*", Proceedings of International Conference on Computers and Devices for Communication, 2009.

[22] S. Parvin, S. Han, F. Hussain and A. Farookh, *"Trust Based Security for Cognitive Radio Networks*", Proceedings of iiWAS 2010, Paris, France, pp. 737-742.

[23] A.B. MacKenzie. *Cognitive networks*, First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks 2005 DySPAN 2005, 2005.

[24] K.-C. Chen, *Trusted cognitive radio networking*, Wireless Communications and Mobile Computing, 2009