Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 7107103, 17 pages
http://dx.doi.org/10.1155/2016/7107103

Research Article

Cognitive Privacy for Personal Clouds

Milena Radenkovic

School of Computer Science, University of Nottingham, Nottingham NG8 1BB, UK

Correspondence should be addressed to Milena Radenkovic; milena.radenkovic@nottingham.ac.uk

Received 24 December 2015; Accepted 3 April 2016

Academic Editor: Chao Chen

This paper proposes a novel Cognitive Privacy (CogPriv) framework that improves privacy of data sharing between Personal Clouds for different application types and across heterogeneous networks. Depending on the behaviour of neighbouring network nodes, their estimated privacy levels, resource availability, and social network connectivity, each Personal Cloud may decide to use different transmission network for different types of data and privacy requirements. CogPriv is fully distributed, uses complex graph contacts analytics and multiple implicit novel heuristics, and combines these with smart probing to identify presence and behaviour of privacy compromising nodes in the network. Based on sensed local context and through cooperation with remote nodes in the network, CogPriv is able to transparently and on-the-fly change the network in order to avoid transmissions when privacy may be compromised. We show that CogPriv achieves higher end-to-end privacy levels compared to both noncognitive cellular network communication and state-of-the-art strategies based on privacy-aware adaptive social mobile networks routing for a range of experiment scenarios based on real-world user and network traces. CogPriv is able to adapt to varying network connectivity and maintain high quality of service while managing to keep low data exposure for a wide range of privacy leakage levels in the infrastructure.

1. Introduction

We live in the era when people expect seamless connectivity for everyone and to everything everywhere. For the majority, this means that potentially personal and sensitive data may get transferred by the networks which can compromise user privacy in different ways [1]. Even though some users may use VPN overlays to improve privacy of their traffic, they will often face difficulties when being mobile or in the areas of intermittent connectivity. This paper addresses the problem of end-to-end privacy in the face of possibly unreliable and mobile networks. We argue that continuously decreasing control that users have on their data needs to be addressed across multiple layers (i.e., not only the application or not only the radio level) and we propose the idea of Personal Cloud architecture that improves privacy of storage as well as sharing of user data. This paper describes an open-source distributed virtual platform that allows adaptive privacy for sharing multiple kinds of data via different routing protocols and networks. In particular, we build on and expand our early work on light weight Personal Clouds demonstration proposed in [2] to allow adaptive and dynamic transfer mechanisms for different types of user traffic based on different traffic privacy levels required. Recent research [3] has shown the wide spread use of transparent middleboxes in cellular networks that actively analyse, monitor, and modify individual's traffic without the knowledge of the individuals and thus compromise their privacy. We propose Cognitive Privacy (CogPriv) which allows different application services (hosted in different virtual containers within Personal Cloud (PC)) to route traffic via most suitable networks in order to avoid network segments that may compromise user privacy and redirect user communication towards more secure networks. For example, if the Cognitive Privacy module in the user's Personal Cloud detects that user's cellular network is likely to spy on them, highly private traffic will be on-the-fly and transparently redirected to local ad hoc networks and follow the more trusted opportunistic ad hoc route to the destination. We propose to integrate several metrics to allow CogPriv routing protocol to probe cellular network trustworthiness and to estimate local ad hoc wireless nodes social dynamics, nodes' trust levels, and resources' availability.

The paper is organised as follows. Section 2 describes the state-of-the-art work on privacy-aware user data communication in mobile networks. Section 3 begins with describing the architecture and design of our light weight Raspberry Pi Personal Cloud testbed. We then move to proposing an opportunistic disconnection tolerant network framework for data forwarding that can on-the-fly adapt to dynamic properties of access points/links and different privacy requirements of user application. The Cognitive Privacy module (CogPriv) of user's Personal Cloud can monitor the local network access points and individually or though collaboration make decisions on the network interface via which to send the data (and whether to send the data) depending on the privacy level required by the application. Section 4 describes CogPriv decision making algorithm and heuristics in more detail. Section 5 provides description of the real world cellular data traces and Facebook users connectivity traces used in our experiments and then moves to describing experiment scenarios and discussing the results. CogPriv shows that it outperform cellular network and mobile social ad hoc network forwarding across a range of metrics. Section 6 gives summary and future work directions.

2. Related Work

In [2], we propose the design and architecture of a low cost Personal Cloud testbed demonstration which uses Raspberry Pi computer and a range of heterogeneous sensors (RasPiPCloud). RasPiPCloud supports multiple on demand virtual containers to host different services and applications that can collect, store and share data with varying different levels of privacy. RasPiPCloud utilizes opportunistic networks communication among itself, heterogeneous sensors and other devices. Figure 1 shows the architecture of the RasPiPCloud with three example LXC containers [4] Healthcare, Finance, and Social Network (with a fourth container template ready for rapid on demand deployment). Each container gets installed and runs its purpose specific applications to ensure secure data fencing and protection.

In [5], the authors identify the widespread use of transparent middleboxes such as HTTP and DNS proxies that are able to analyse and actively modify user traffic and thus compromise user privacy and security. The authors argue that it is very important to consider higher-layer relationships when seeking to analyse mobile traffic and illustrates how mobile operators can enforce the use of HTTP proxies and gateways through preconfigured APN (Access Point Name) settings on a device. They identify that typical users lack the mechanisms and knowledge to prevent operator-enforced proxies from performing header injection and to stop online services from collecting their information. The reliance on VPN is limiting in cases of mobile or disconnection prone scenarios. Our paper addresses these scenarios by proposing a way how our combined intelligent routing may exploit maximally trusted routes based on the real time probes and collaboration with the infrastructure or ad hoc local nodes.

In [3], authors consider cellular networks where the growth of capacity provision is still behind the user and application demands [6]. Because of this, mobile network operators increasingly use auxiliary networks (e.g., WiFi networks) to offload mobile traffic for additional capacity. In recent years, WiFi offloading has been rapidly emerging as the preferred technique to meet the needs. Other research has addressed WiFi offloading efficiency [7, 8], energy efficiency [9, 10], user incentives [11] and operator support [12, 13]. Reference [3] focuses on improving the balanced control of WiFi offloading and avoid poor network utilization and undesirable user experience [9, 14] by proposing SoftOffload that aims to enhance deployability and collaboration among mobile network operators, WiFi providers and mobile users. SoftOffload employs collaborative hierarchical design between its central controller and local agents in order to balance between global control and responsiveness at the network edge.

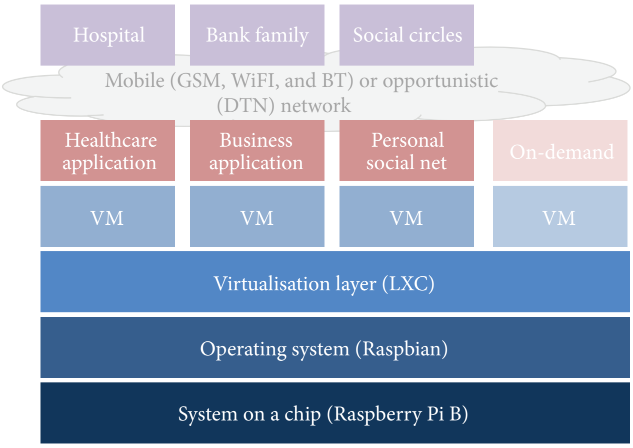

Hospital
Bank family
Social circles
Mobile (GSM, WiFI, and BT) or opportunistic (DTN) network
Healthcare application
Business application
Personal social net
On-demand
VM
VM
VM
VM
Virtualisation layer (LXC)
Operating system (Raspbian)
System on a chip (Raspberry Pi B)

Figure 1: RasPiPCloud architecture.

In [15] authors propose cognitive testbed for wireless sensor networks as an emerging technology with a vast potential to avoid traditional wireless problems such as reliability, interferences and spectrum scarcity in wireless sensor networks. In addition to the testbed, [15] also proposes the design of a cognitive simulator for networks with a high number of nodes and the implementation of a new platform with three wireless interfaces and cognitive software for extracting real data.

State of the art work in [16] proposes Haystack system which aims to allow unobtrusive and comprehensive monitoring of network communications on mobile phones entirely from user space. Haystack correlates disparate contextual information such with specific traffic flows destined to illuminate mobile phone app performance, privacy and security.

Authors in [5] use data collected by the Netalyzr network service over 16 months to identify and characterize HTTP header enrichment in modern mobile networks. They present an overview of HTTP header usage for 299 mobile service providers from 112 countries to show three main categories: unique user and device identifiers, headers related to advertising programs, and headers associated with network operations which present significant compromise to user privacy. In our paper, we use traces of 17 mobile service providers of one country provided in this dataset with real world social network connectivity traces.

Reference [17] identify that typical privacy preserving solutions for data analysis which utilise cryptographic algorithms introduce high computation costs or restrict the possible range of values due to the need of discrete logarithm computation. Reference [18] propose a solution with a fully trusted dealer which may not be suitable for real world applications due to increased communication overheads necessary for their static key management scheme. Emerging work in [19] proposes to eliminate the need for key redistribution following a user join or leave as well as the need for fully trusted key dealer thus moving to a more P2P paradigm which is core to our approach too.

In [20, 21] we propose a new P2P adaptive anonymity technique for mobile opportunistic networks that improves traditional competitive research which is not well suited to sparse and disconnection prone networks. Reference [22] propose opportunistic, adaptive, fully localized reputation aware obfuscation mechanism that comprises of collaborative testing of nodes' obfuscation behaviour (OCOT) and multidimensional adaptive anonymisation (AA). We show that OCOT-AA is very efficient in terms of achieving high levels of node identity obfuscation and managing low delays while enabling fast detection and avoidance of malicious nodes. This paper moves beyond this to propose Cognitive Privacy for Personal Clouds with multiple application domains.

3. Cognitive Privacy and Personal Clouds

3.1. Personal Cloud: Prototype Testbed and Architectural Overview. Increasing demand for using a range of applications with different privacy requirements on mobile handheld devices raises challenges of how to choose the network (i.e., network interface) with the most suitable levels of privacy. We argue that handheld cognitive devices with several heterogeneous network interfaces (e.g., cellular networks, wireless networks, ad hoc wireless, and Bluetooth) are core for supporting a range of applications with different privacy requirements hosted in different virtual containers [2]. For example, consider a user who can be running a social network that allows them to stay in contact with their friends at the same time as regularly monitoring their long-term medical condition and being in contact with the hospital. These two types of applications have different privacy requirements and need their data to be stored and shared in different ways that can adapt to the required privacy requirements dynamically. We refer to this as Personal Cloud [2] which is in line with the proposals described in [23, 24]. Figure 2 shows deployment of a Personal Cloud prototype demo on a Raspberry Pi device equipped with Xtrinsic sensor board comprising temperature, pressure, and acceleration sensors. Figure 3 shows Raspberry Pi device that captures, stores, and processes a range of user and environment data such as heart rate and pedometer. Figure 4 shows a dashboard visualisation of the heart rate sensor readings and Figure 5 shows a social network hosted by the user and displayed on the user's handheld device.

This paper expands on the idea in [2, 23] in several ways in order to enable reliable and adaptive data sharing.

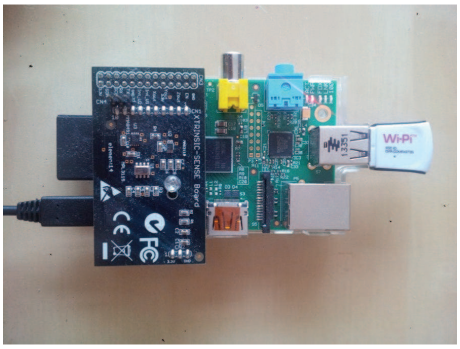


Figure 2: Raspberry Pi B with Xtrinsic sensor board and a WiPi wireless adapter.

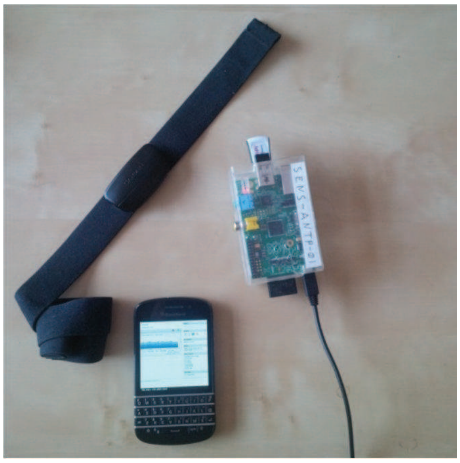
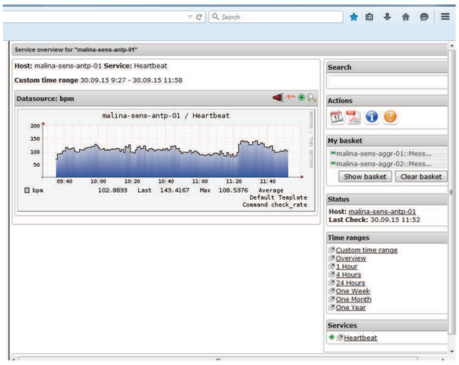


Figure 3: Raspberry Pi with Suunto and WiPi USB module, Garmin heartrate sensor, and smartphone displaying readings.



Service overview for "malina-sens-antp-01"

Host: malina-sens-antp-01 Service: Heartbeat

Custom time range 30.09.15 9:27 - 30.09.15 11:58

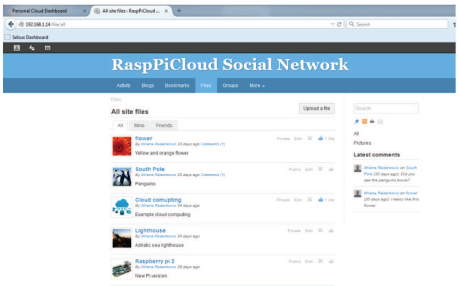
Datasource: bpm

bpm 102.8833 Last 143.4167 Max 108.5376 Average
Default Template
Command check_rate

Status
Host: malina-sens-antp-01
Last Check: 30.09.15 11:52

Figure 4: Visualisation of heart rate readings from the Garmin sensor.

While some social media data can be transferred via cellular network independently of whether there are middleboxes present in transit, medical personal data requires higher level of privacy that should not be compromised nor should it be allowed that the frequency and patterns of communication to the hospital are gathered by the cellular network provider infrastructure. Figure 6 shows a Personal Cloud



All site files

flower
By Milena Radenkovic 33 days ago Comments (1)
Yellow and orange flower

South Pole
By Milena Radenkovic 33 days ago Comments (1)
Penguins

Cloud comupting
By Milena Radenkovic 34 days ago
Example cloud computing

Lighthouse
By Milena Radenkovic 34 days ago
Adriatic sea lighthouse

Raspberry pi 2
By Milena Radenkovic 35 days ago
New Pi version

Latest comments

Milena Radenkovic on South Pole (30 days ago): Did you see the penguins movie?

Milena Radenkovic on flower (30 days ago): I really like this flower

Figure 5: RasPiPCloud personal social network.

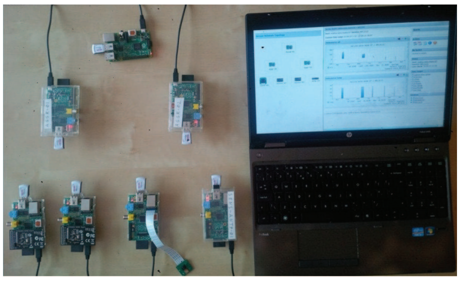


Figure 6: Testbed architecture and visualisation.

prototype demo utilising multiple Raspberry Pis where the leaf Raspberry Pis with heterogeneous sensors aim to send their data (camera and heart rate) to the hub destination node via different routes. Intermediary nodes may have different privacy levels associated with them. Nodes are configured so that leaf nodes have connectivity to intermediary nodes but not directly to destinations. This is important as it allows us to test multiple Personal Clouds communications over variable network conditions and topologies. Note that all nodes are equipped with WiPi wireless adapters that support both infrastructure and ad hoc mode.

3.2. Cognitive Privacy. In this section, we describe how we extend our early work on Personal Cloud testbed [2] to include transparent, efficient, and adaptive Cognitive Privacy (CogPriv) which negotiates access to various networks in real time to suit the privacy requirements of the applications. One of the core building modules of the Cognitive Privacy framework is Intelligent Forwarder which is a P2P DTN module. We extend the DTN bundle protocol (RFC 5050 [25–27]) which provides API for DTN applications with intelligent P2P forwarding. More specifically, our P2P DTN intelligent forwarding module provides multiflow real time bundle forwarding based on a range of criteria such as source ID, Virtual Machine (VM) ID, application privacy requirements, and destination ID so that different incoming bundles can be matched to the appropriate network interface in real time. Additionally, CogPriv comprises the following multiple stages: it probes local cellular network to identify the likelihood of any middleboxes that may compromise user traffic, requests the remote destination nodes to provide their estimations of the cellular network privacy levels, and collaborates and cooperates with the local network nodes. In this way, CogPriv can range dynamically and adaptively from providing fully cellular single hop end-to-end communication to fully localised multihop mobile opportunistic communication.

Intelligent Forwarder makes the decision on the choice of the next forwarding node and network interface based on multiple criteria and objectives: (1) it aims to either maximise end-to-end privacy for a particular application or meet the requirements of the application, (2) it aims to minimise end-to-end delays, and (3) it aims to be resource aware and adaptively avoid congestion. In this way, Intelligent Forwarder manages privacy requirements while being aware and adaptive to the dynamic quality of service challenges.

Through collaborations and cooperation in the local neighbourhoods, each node aims to understand its environment better and learn about its neighbours. More specifically, each node exchanges the following: (1) their own cellular network privacy statistics and predictions to negotiate feasibility of using cellular network for a particular application, (2) predictive analytics of their resources, and (3) mobile social graph network connectivity analytics. Social connectivity analytics is important as it keeps directionality of the data to be routed for ad hoc opportunistic communication. Resource considerations are important as they enable higher reliability of ad hoc opportunistic routing. More specifically, CogPriv builds on implicit heuristics on predictive in-network storage and delays we proposed in [28–31].

Each node's privacy level estimations are important to consider as they are the core criteria for choosing the interface to use for forwarding the data for privacy-aware applications; that is, neighbouring nodes may communicate via WiFi, GSM, or Bluetooth each having different privacy levels. More specifically, each interface will have different probabilities and utilities associated with it (described in Section 4) so that each bundle can be forwarded via the most appropriate interface. Towards this goal, we extend simple static (interface and bundle) forwarding paradigm to the more dynamic (interface, bundle, and forwarding probability) paradigm. Figure 7 shows Personal Cloud extended with the CogPriv framework.

3.3. An Overview of Cognitive Privacy Distributed Decision-Making. Depending on the level of privacy an application requires, the Cognitive Privacy (CogPriv) module in the Personal Cloud will send the data via either cellular network (e.g., default for mobile phones) or WiFi (e.g., default for laptops) when privacy is not required; on the other hand, it will run probes on its local area network and communicate with the destination about the remote cellular network privacy levels, as well as collaborating with the nearby nodes before deciding via which network and next hop to send the data as shown in Figure 8.

These steps are described in more detail as follows:

(i) If the desired privacy level is high, the Personal Cloud first checks its cellular network by running probes to identify possible presence of middleboxes. If it discovers any, it does not use cellular network.

(ii) If the cellular network of the sender does not detect presence of middleboxes, the sender contacts

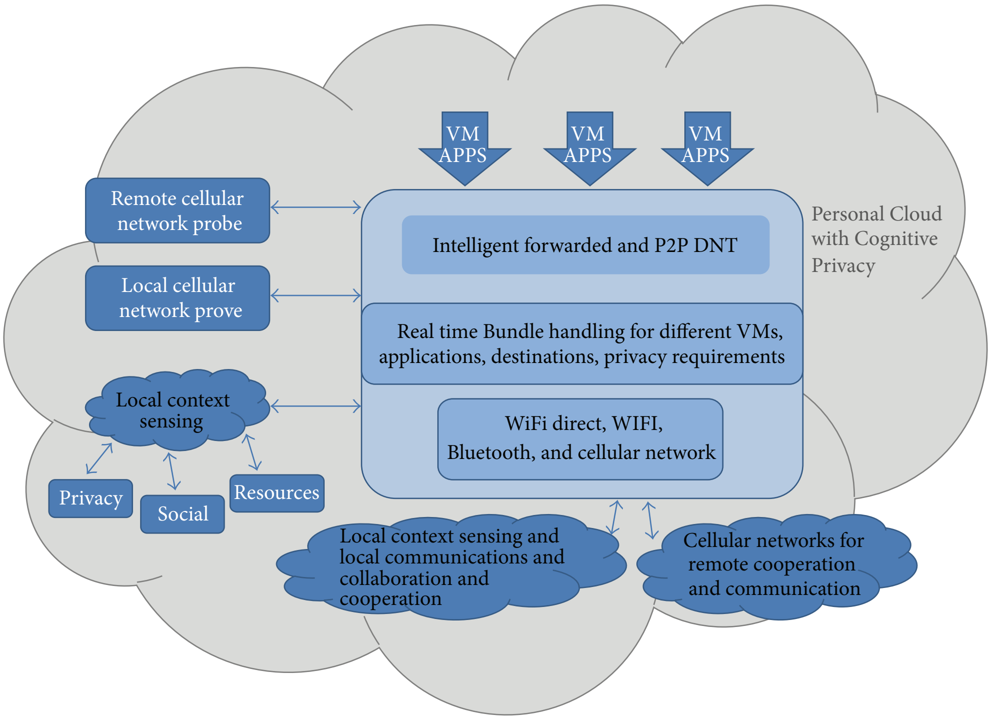

VM APPS
VM APPS
VM APPS
Remote cellular network probe
Local cellular network prove
Intelligent forwarded and P2P DNT
Personal Cloud with Cognitive Privacy
Real time Bundle handling for different VMs, applications, destinations, privacy requirements
Local context sensing
WiFi direct, WIFI, Bluetooth, and cellular network
Privacy
Social
Resources
Local context sensing and local communications and collaboration and cooperation
Cellular networks for remote cooperation and communication

Figure 7: Cognitive Privacy design for Personal Clouds.

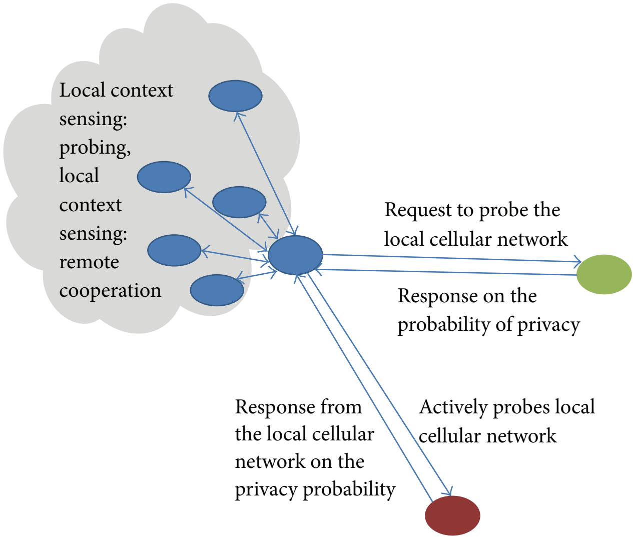

Local context sensing: probing, local context sensing: remote cooperation
Request to probe the local cellular network
Response on the probability of privacy
Response from the local cellular network on the privacy probability
Actively probes local cellular network

Figure 8: Functional overview of the probing and local collaboration stages.

the destination to enquire if the destination can detect any middleboxes at their end.

(iii) If both the destination and the sender are clear of the middleboxes or the level of middleboxes privacy meets the application requirements, the data gets communicated via the cellular networks.

(iv) If either the destination or the sender is not clear of infrastructure middleboxes, the sender checks its local neighbourhood using ad hoc networks and local contacts with trusted nodes only (for high levels of privacy requirements) and WiFi for medium levels of privacy requirements.

(v) If the next hop node gets a bundle with high level of privacy requirements, it will first probe its cellular network and send the bundle via it only if its cellular network does not have any middleboxes detected. Otherwise, it will scan opportunistically its local nodes and will exchange its social, resource, and privacy matrix in order to determine which node may be the most suitable bundle carrier to the particular destination.

(vi) For each bundle carrier, the same set of steps gets preformed in a fully distributed manner at every node.

Figure 9 illustrates combined, diverse communication approaches that comprise CogPriv and Figure 10 gives architectural overview of CogPriv.

A key challenge that CogPriv solves regarding cellular-local switching is that valuable middlebox and contextual information are distributed across local and remote users. The irregular distribution means that the contextual information possessed by any node alone is not sufficient to guide the switching process. Cellular network infrastructure can vary with the location of access and times users use the network so that different middleboxes may be present or removed without user's knowledge. For example, a Vodafone user in Karsruhe can send traffic without it being intercepted by a middlebox, while a Vodafone user in Berlin might pass via a web cache middlebox. Similarly, a T-Mobile user at a given

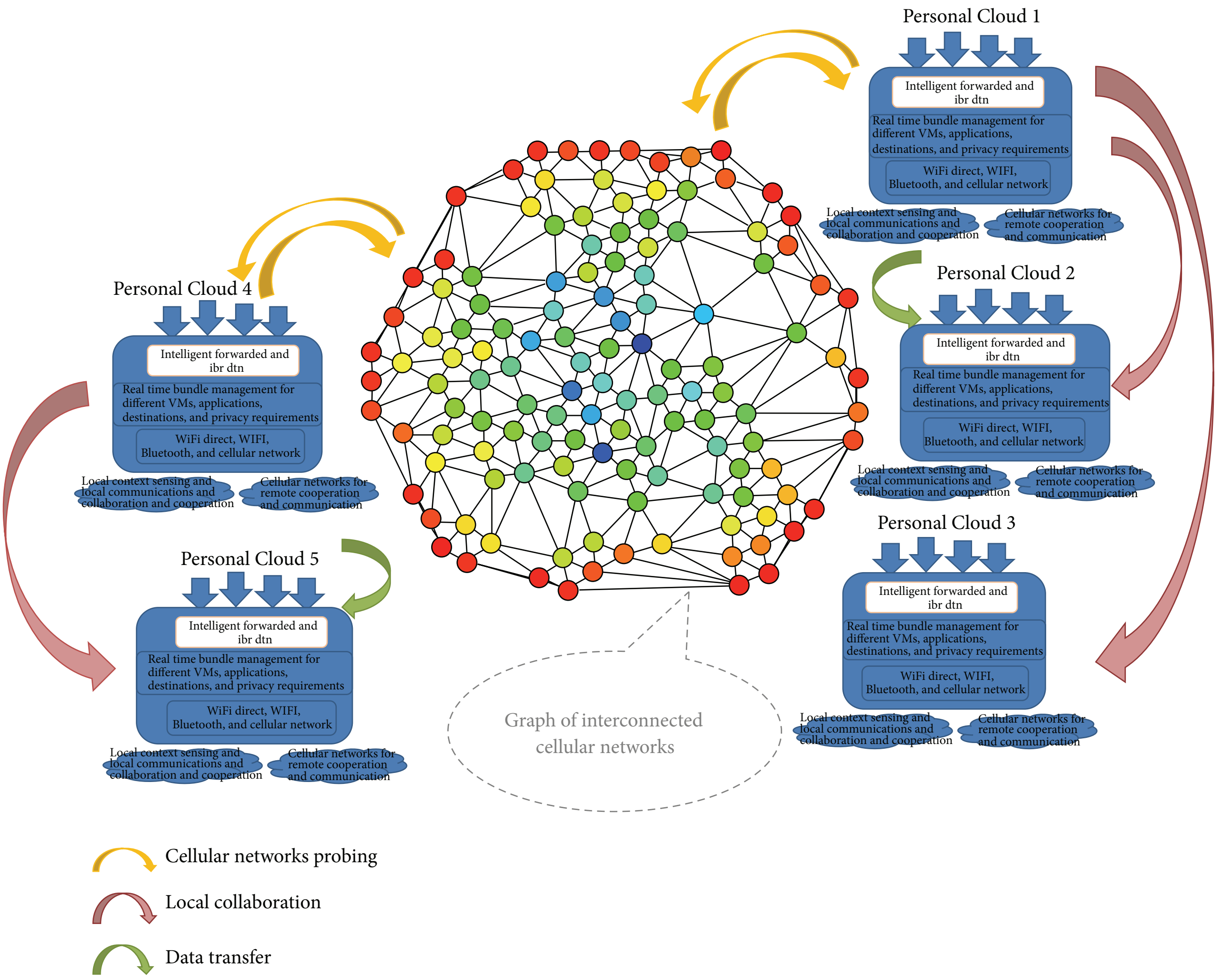

Personal Cloud 1
Intelligent forwarded and ibr dtn
Real time bundle management for different VMs, applications, destinations, and privacy requirements
WiFi direct, WIFI, Bluetooth, and cellular network
Local context sensing and local communications and collaboration and cooperation
Cellular networks for remote cooperation and communication
Personal Cloud 2
Intelligent forwarded and ibr dtn
Real time bundle management for different VMs, applications, destinations, and privacy requirements
WiFi direct, WIFI, Bluetooth, and cellular network
Local context sensing and local communications and collaboration and cooperation
Cellular networks for remote cooperation and communication
Personal Cloud 3
Intelligent forwarded and ibr dtn
Real time bundle management for different VMs, applications, destinations, and privacy requirements
WiFi direct, WIFI, Bluetooth, and cellular network
Local context sensing and local communications and collaboration and cooperation
Cellular networks for remote cooperation and communication
Personal Cloud 4
Intelligent forwarded and ibr dtn
Real time bundle management for different VMs, applications, destinations, and privacy requirements
WiFi direct, WIFI, Bluetooth, and cellular network
Local context sensing and local communications and collaboration and cooperation
Cellular networks for remote cooperation and communication
Personal Cloud 5
Intelligent forwarded and ibr dtn
Real time bundle management for different VMs, applications, destinations, and privacy requirements
WiFi direct, WIFI, Bluetooth, and cellular network
Local context sensing and local communications and collaboration and cooperation
Cellular networks for remote cooperation and communication
Graph of interconnected cellular networks
Cellular networks probing
Local collaboration
Data transfer

FIGURE 9: Cellular network interactions with local Personal Clouds.

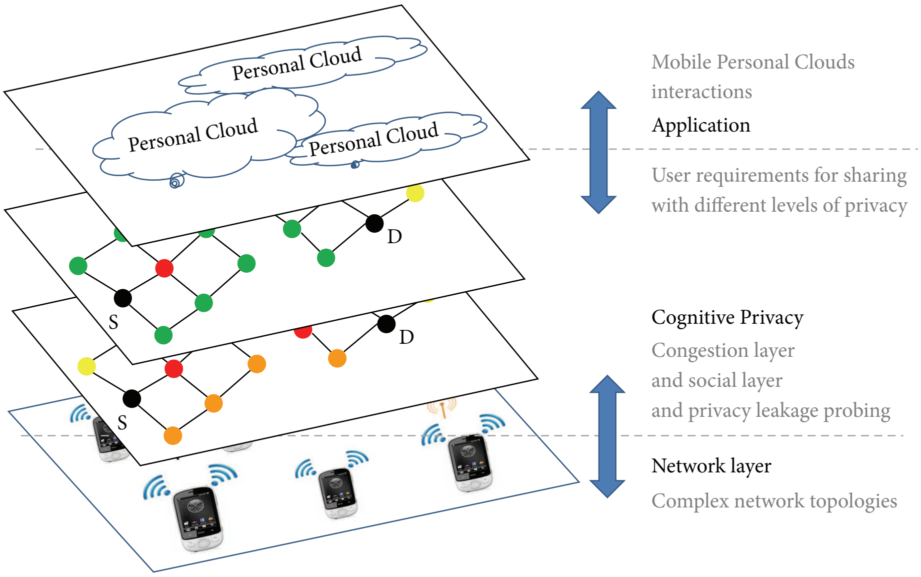

Personal Cloud
Personal Cloud
Personal Cloud
S
D
S
D
Mobile Personal Clouds interactions
Application
User requirements for sharing with different levels of privacy
Cognitive Privacy
Congestion layer
and social layer
and privacy leakage probing
Network layer
Complex network topologies

FIGURE 10: Architectural overview of Cognitive Privacy.

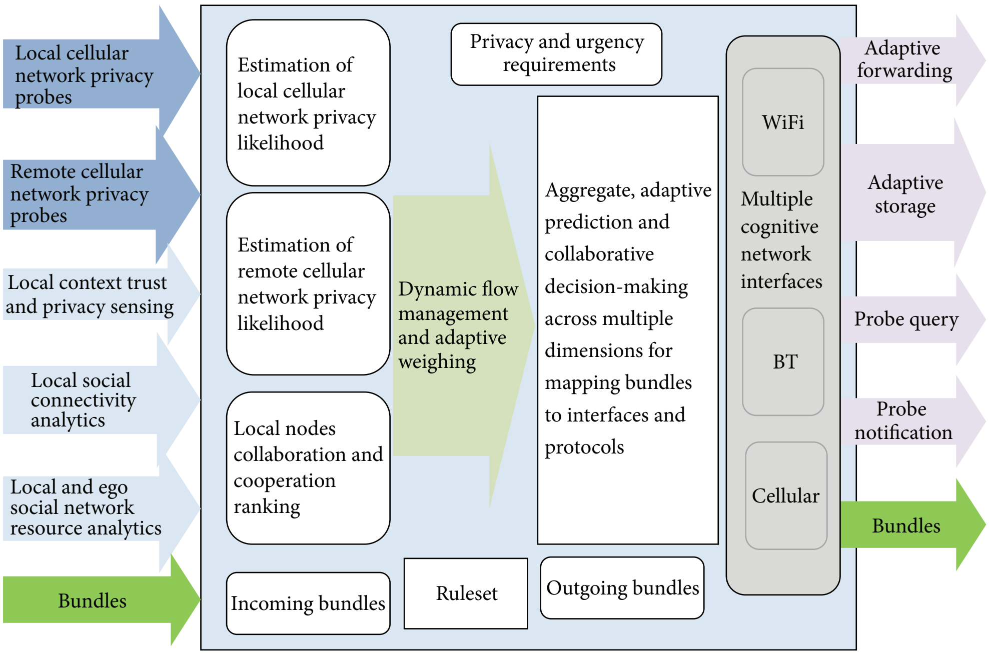

Local cellular network privacy probes
Remote cellular network privacy probes
Local context trust and privacy sensing
Local social connectivity analytics
Local and ego social network resource analytics
Bundles
Estimation of local cellular network privacy likelihood
Estimation of remote cellular network privacy likelihood
Local nodes collaboration and cooperation ranking
Incoming bundles
Ruleset
Outgoing bundles
Privacy and urgency requirements
Dynamic flow management and adaptive weighing
Aggregate, adaptive prediction and collaborative decision-making across multiple dimensions for mapping bundles to interfaces and protocols
Multiple cognitive network interfaces
WiFi
BT
Cellular
Adaptive forwarding
Adaptive storage
Probe query
Probe notification
Bundles

FIGURE 11: Architectural overview of the decision-making in the Personal Cloud Cognitive Privacy module.

VM ID	App ID	SRC ID	Privacy required	Personal Cloud contact list	Probe Local Estimation	Probe Remote Estimation	Betweeness	Tie strength	Resources

FIGURE 12: Extended CogPriv bundle header format.

location using 4G might detect a web middlebox, while a T-Mobile user on 3G could identify a DNS middlebox.

Because both the number and the location as well as the functionality of the middleboxes in cellular networks can change randomly, the cellular network probes need to be performed either before each data transfer (which may increase control traffic especially for real time multimedia traffic) or each sensible time interval (e.g., every day or half a day). Based on the statistical and temporal analysis of the probes each node performs for different cellular networks, nodes can adjust their time intervals differently so that they perform probes for some networks more frequently than for others.

In Figure 11, we show that after estimating the privacy levels of local and remote nodes they get ranked via the Ruleset as well as privacy and urgency requirements. Each flow is dynamically managed to enable adaptive weightings of the input parameters. CogPriv then maps the incoming bundles to suitable outgoing interfaces and protocols. Possible decisions that CogPriv can take include adaptive forwarding (choosing the best hop), adaptive storing (choosing to retain the bundle), probe query (issuing the query on behalf of another node), responding to query when being asked.

4. Cognitive Privacy Algorithm and Decision Heuristics

In this section, we propose and describe several new heuristics for driving local collaborative decisions and discuss in detail cooperative probing mechanism as integral and complementary parts of CogPriv.

Cooperative CogPriv module includes intelligent dynamic probing of the local cellular network for any privacy threatening middleboxes and cooperation with the destination about its cellular network. The results of these probes are stored in two fields (Probe Local Estimation and Probe Remote Estimation) as part of extension of the bundle header format referred to as Extended CogPriv bundle header format shown in Figure 12.

Collaborative CogPriv module uses several metrics for heuristics and analytics of ad hoc neighbours privacy levels in order to predict the level of privacy each node can provide. More specifically, each node generates information on its estimated privacy level and exchanges it with its neighbours. The Extended CogPriv bundle header contains information on node social and resource metrics: betweenness, tie strength, and resources as shown in Figure 12.

Adaptive forwarding decision (InfrastructureprivUtil) is a function of estimated local and remote privacy as well as collaboration involving message exchange on these estimations (formula (1)). In addition to the exchange of measurements of local privacy levels (LocalProbUtil) collaboration involves QoS metrics in order to achieve maximum quality of service in terms of minimal delays and minimal resource overload while achieving maximum required privacy. This is shown in formula (2). Consider

$$\text{InfrastructureprivUtil} = f\left(\text{local\_cell\_probe, remote\_cell\_probe}\right), \quad (1)$$

$$\text{LocalProbUtil} = f\left(\text{local\_cell\_probe, social analytics, resource analytics, cooperation}\right). \quad (2)$$

Therefore, the headers need to include in-network delays prediction, in-network storage, social betweenness, centrality, and tie strengths with the destination in order to allow bundles to keep directionality of the sent bundles, as shown in the following:

$$h \in H = \{w_1 * \text{Priv}, w_2 * (\text{Ret, Rec}), w_3 * \text{social}\}, \quad (3)$$

where w_1 is weight that depends on the privacy requirements identified for this traffic type, w_2 is the weight of the local resource estimation, and w_3 is the weight of the local social estimation.

When a forwarding node (X) meets contacts on its way, it exchanges relevant heuristics and calculates the CogPrivUtil of each contact. This is shown in formulas (4) and (5). The CogPrivUtil allows the node X to detect how well connected its contact Y is and how available Y is in terms of estimated privacy levels it supports, storage, delay, and social connectivity parameters.

Formula (5) proposes new metric ($\text{Util}_{\text{Priv}}$) for calculating relative utility of the infrastructure privacy ($\text{Infrastructure}_{\text{priv}}$) when compared to the local privacy ($\text{Local}_{\text{priv}}$):

$$\text{CogPrivUtil}_D(X) = \sum_{h \in H} w_h \text{Util}_h(X), \quad (4)$$

$$\text{Util}_{\text{Priv}}(X) = \frac{h\left(\text{Infrastructure}_{\text{priv}}(X)\right)}{h\left(\text{Infrastructure}_{\text{priv}}(X)\right) + h\left(\text{Local}_{\text{priv}}(X)\right)}. \quad (5)$$

Retentiveness (Ret) [28–31] refers to the node's available storage for the new bundles that are sent to them. Retentiveness is an important attribute to consider because of the store and forward nature of opportunistic DTN networks [32]. Nodes with limited storage, either due to popularity or simply due to Personal Cloud hardware constraints, are more susceptible to bundle loss. Retentiveness is calculated as an exponentially weighted moving average of a Personal Cloud remaining storage. Formula (6) shows that retentiveness of X is calculated as the sum of all bundle occupancy subtracted from the node's buffer capacity ($B_c(X)$):

$$\text{Ret}(X) = B_c(X) - \sum_{i=1}^{N} b^i_{\text{size}}(X). \quad (6)$$

Receptiveness (Rec) [28–31] refers to the Personal Clouds' ability to receive bundles and forward them on. This is an important observation as increasing in-network delays is an indication that the volume of traffic a node or region is receiving is greater than the bandwidth available to it for offloading. The delay between receiving a bundle and forwarding a bundle is constrained by the size of the buffer and the bandwidth available for a node to offload the bundles. Nodes with large size of storage are more susceptible to receiving more bundles than being capable of offloading. Formula (7) shows that receptiveness is the total current bundle delay, calculated as the sum of differences between the current time (T_{now}) and the time each bundle was received (M_{received}):

$$\text{Rec}(X) = \sum_{i=1}^{N} \left(T_{\text{now}} - b^i_{\text{received}}(X)\right). \quad (7)$$

Each node keeps track of its centrality degree defined as the number of its encounters during predefined time and betweenness defined as the existing indirect links between each pair of its neighbours.

Degree is computed as total number of direct links to a given user n:

$$C_D(n_0) = \sum_{k=1}^{N} a(n_0, n_k). \quad (8)$$

Related work on online social networks [33] presents large-scale study of fine grained privacy preferences for Facebook users which provides the information on how users specify social access control lists (SACL) on a social networking service. They show that SACL membership has little correlation with profile information and online social network links; and making recent SACLs available to users is more promising as users tend to reuse SACLs. We expand on these findings and propose to use the recency, betweenness, and frequency social metrics for choosing the more trusted data carriers as suitable for mobile (disconnection prone) social networks.

We define betweenness in line with [34] by building and processing adjacency matrix. The adjacency matrix is updated based on the application requirements:

$$C_B(p_i) = \sum_{j=1}^{N} \sum_{k=1}^{j-1} \frac{g_{jk}(p_i)}{g_{jk}}. \quad (9)$$

Frequency refers to the number of times a given user n encounters a destination d. Frequency graph of user n to the destination d is calculated as follows:

$$F_n(d) = \frac{f(d)}{F(n) - f(d)}, \quad (10)$$

where $f(d)$ is the number of times destination d has been encountered and $F(n)$ is the total time that user n has encountered d from the beginning of the simulation.

Recency is defined as how recently a user n last met a destination d shown in the following:

$$\text{Recency}_n(d) = \frac{\text{recency}(d)}{T(n) - \text{recency}(d)}. \quad (11)$$

Tie Predictor. Once a user encounters destination, it computes the similarity to the destination and updates. More specifically, the similarity refers to the number of direct neighbours and indirect encounters. The higher the number of common neighbours is, the higher the probability that a given user moves regularly to this destination is. To account for more synchronous communication, we use similarity as a core metric for calculating tie prediction:

$$\begin{gathered}\text{TsUtil}_n(m) = \frac{\text{TS}_m(d)}{\text{TS}_m(d) + \text{TS}_n(d)}, \\ \text{SimUtil}_n(m) = \frac{\text{Sim}_m(d)}{\text{Sim}_m(d) + \text{Sim}_n(d)}.\end{gathered} \quad (12)$$

Choosing Carrier. The decision on forwarding of the stored bundle is based on the utility calculation whenever a source or a carrier detects a new neighbour. If the new neighbour has a higher total utility compared to the given user, the bundle will be forwarded. The utilities are computed by pairwise comparison:

$$\text{CogPrivUtil}_n(m) = \frac{\text{CogPriv}_D(m)}{\text{CogPriv}_D(m) + \text{CogPriv}_D(n)}. \quad (13)$$

5. Experiment Setup and Results

5.1. Experiment Scenario and Datasets. We begin with describing two real-world data traces that we use in our experiments and then describe our methodology of running experiments and clarify our criteria before we give and discuss our results.

We base our experiments on the real-world data traces of different probes for mobile networks across 112 countries and over 200 mobile providers obtained by Netalyzr in [1]. Examples of the probes in [1] include Web probes such as *http_content_change*, *http_hdr_reorder*, *http_hdr_injection*, *invalid_host_name_vulnerability*, *http_enforcement*, *http_default_compression,* and *Transcoding* as well as DNS probes which include *dns_direct_mangled*, *dns_direct_proxy*, and *dns_direct_changed_id*.

We select traces of one country (Germany) as its number of mobile networks' providers best suits our real-world user communication trace [35] so that every user can be on the different network. For every mobile node, we obtain the probability for the network spying on the web traffic by calculating the percentage of test returning positive versus the total number of tests performed. For every mobile network, we obtain the probability of it spying on web traffic by averaging the values obtained by all individual mobile nodes on this particular network.

Table 1: Overview of middlebox distribution identified in a range of mobile providers in Germany.

Name	Probes	Web	DNS	Web %	DNS %
1&1	1	1	0	100	0
ALICE	1	0	0	0	0
BASE	12	0	12	0	100
BLAU	3	0	3	0	100
CONGSTAR	6	6	3	100	50
DEBITEL	1	0	1	0	100
E-PLUS	9	0	9	0	100
FONIC	1	0	1	0	100
FYVE	5	5	3	100	60
KABELBW	1	0	1	0	100
LIDL	2	0	0	0	0
MEDION	5	0	5	0	100
M-NET	2	0	1	0	50
NETZCLUB	1	0	0	0	0
O2	35	0	16	0	45.71429
T-Mobile	83	83	27	100	32.53012
Vodafone	36	36	10	100	27.77778

The table of mobile networks, probes, and analysis is given in Table 1.

We carry out performance evaluation of CogPriv versus cellular communication and local social opportunistic networks across a range of network conditions and user traffic types across a range of metrics.

Based on the real cellular networks in Germany (shown in Table 1), we average privacy levels into five evenly distributed privacy threat levels, for example, minimum (0%) such as ALICE and NETZCLUB, low (25%) such as M-NET, medium (50%) such as BASE and MEDION, high (75%) such as CONGSTAR, and maximum (100%) such as FYVE.

We developed extensions to the one simulator [36] that utilises data from Table 1 in order to return middleboxes presence probability discovered when performing probing of different cellular networks.

We run experiments with the entire time of real-world Facebook connectivity traces UNICAL [35] for maximum privacy requirements with five different levels of cellular network privacy to which users are connected. UNICAL contains Bluetooth device proximity data, collected by an ad hoc Android application, and the social profiles in terms of Facebook friendships and interests of a group of 15 students. Experimental data were collected at the campus of University of Calabria in Rende, Italy. In order to gather the proximity information, the aforementioned ad hoc application was installed on each student's smartphone. Each participant was instructed to keep with themselves the device that ran the SocialBlueConn application. The experiment lasted one week during student's lessons, from January 28, 2014, to February 5, 2014, including only the working days. Unlike [37, 38] traces, [35] does not identify beginnings and ends of contacts but only sightings. We have assumed that the sightings last at least 60 seconds based on the interval duration between the most frequent sightings. Detailed analysis of mobile social networks and online social networks for UNICAL has been done in [35] and has shown high degree correlation which we exploit in our ad hoc local message forwarding in our experiments.

We assume that all sending nodes aim to send highly personal but not urgent messages (e.g., self-monitoring ongoing long-term health conditions) for large number of experiments, but we also investigate CogPriv performance in the face of varying privacy requirements. We assign varying privacy requirements to each bundle and each CogPriv node can check if the reported levels of middlebox presence in the network can be tolerated for each bundle based on the comparison of levels of middleboxes and privacy required.

In our experiments, we measure end-to-end achieved privacy levels, end-to-end delays, and number of hops between the end points. We run extensive experiments in three increments with steps of 4 (26% of all nodes), 8 (48% of all nodes), and 12 (80% of all nodes) which we repeat for 5 randomly selected combinations of sources and receivers for each cellular network privacy level. This is important for allowing us to get medium, minimum, maximum, and average for each metric. Our results showed that there are no significant differences between different percentages of nodes actively generating and sharing content for the privacy related metrics. We provide Figure 13 to show this. Regarding the resource metrics (retentiveness), we give Figure 19 that focuses on exploring differences between wide range of sending nodes and privacy requirements. Figure 19 does not show significant resource availability differences due to CogPriv utilising an effective congestion aware forwarding heuristics on retentiveness and receptiveness introduced in [28–31].

The following results show that adaptive Cognitive Privacy approach is fundamental for future pervasive applications where Personal Clouds need to communicate via different levels of network privacy for different applications. CogPriv module that is adaptive, real time, collaborative, and cooperative is the core component of future Personal Clouds and necessary extension of the virtualisation of the application storage and hosting. We show that CogPriv is able to gracefully and transparently adapt to local context (both social and network) and remote context (via probes and communication with the destination).

5.2. Results

5.2.1. Achieved End-to-End Privacy and Analysis. Figure 13 shows that end-to-end privacy levels remain higher for CogPriv approach than for cellular only and mobile social ad hoc communication independently of the level of presence of middleboxes in the cellular infrastructure, that is, ranging from no middleboxes to wide range of middleboxes; the performance of Cognitive Privacy drops from 100% privacy level to 85%. This is in contrast with the cellular network which drops end-to-end privacy linearly with the amount of the middleboxes in the cellular network. CogPriv approach also outperforms fully local social ad hoc approach because of the delays that are associated with the bundles time-out and invoke the nodes to utilise cellular infrastructure that may have privacy leaks.

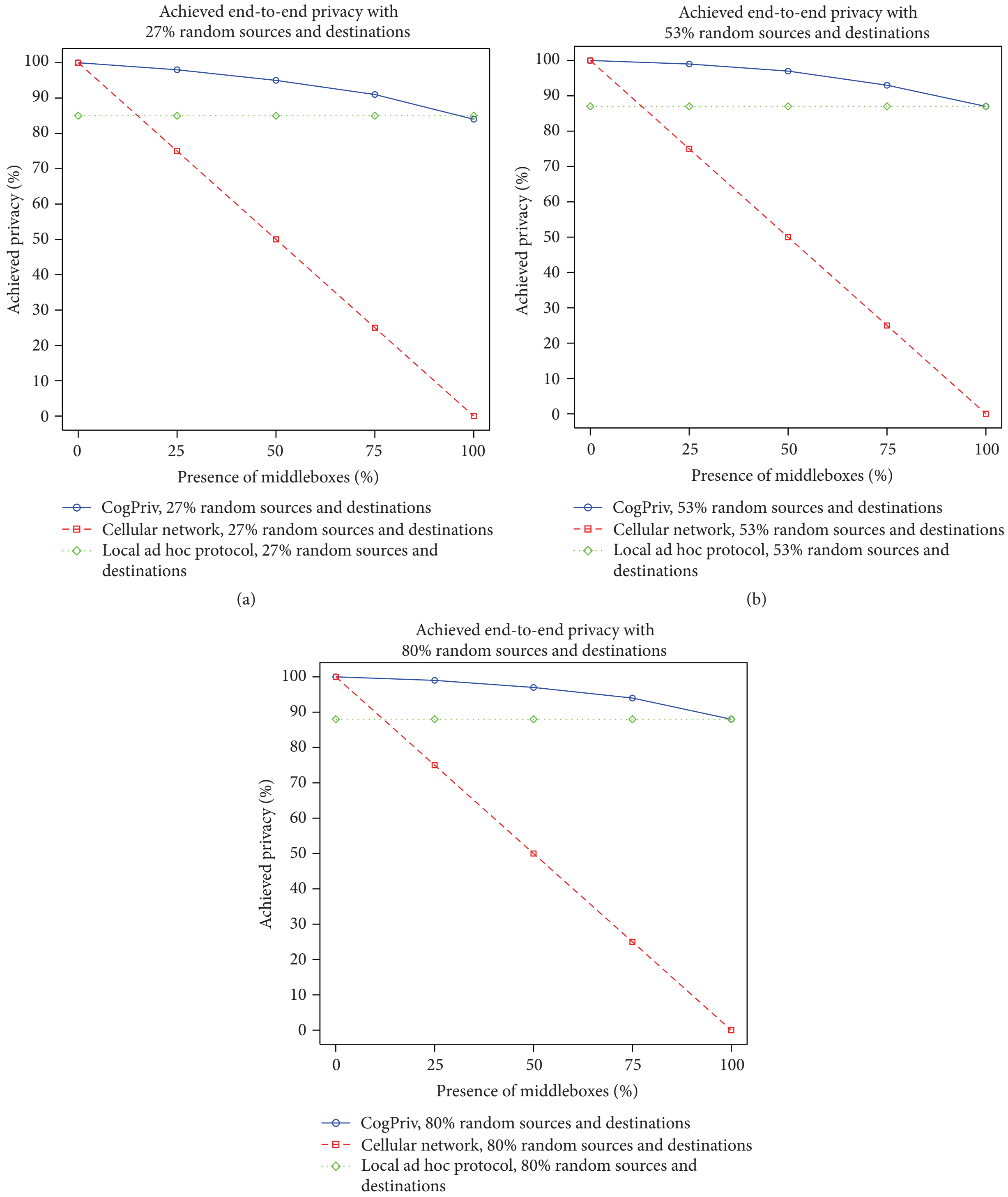
In order to cover wide range of nodes and more conditions they may face (e.g., not to miss a node or nodes that are disconnected), we have done performance analysis for 27% (4 nodes out of 15), 53% (8 nodes out of 15), and 80% (12 nodes out of 15) of randomly selected nodes acting as senders and receivers and each experiment run has been repeated 5 times. We show that there are very minor differences in the performance in the three graphs in Figure 13. Figure 13 shows constant achieved end-to-end privacy for local ad hoc routing for each random selection of senders/receivers. This is due to the use of the real-world trace where the conditions in the node connectivity among the selected nodes do not change for one selection of the nodes for one experiment run as well as due to ad hoc local not detecting middleboxes in the cellular infrastructure and thus not changing its behaviour in the face of the increasing levels of middleboxes.

From Figures 13(a), 13(b), and 13(c), we can see that the differences in E2E privacy for local ad hoc network may slightly change for different numbers of senders and receivers but this difference is also low. This is due to the trace having strong mobile social network characteristic (as it is based on the real-world students traces) and us using local ad hoc routing which exploits social connectivity patterns for forwarding.

Figure 14 shows statistical analysis of end-to-end privacy levels for bundles (mean, max, and min) for different levels of presence of middleboxes in the cellular networks. We observe that there are no drastic oscillations in the level of end-to-end privacy and quality of services for the end-to-end nodes. This is because CogPriv approach adapts very effectively and is able to optimally utilise both local and infrastructure resources.

In order to better understand the influence on end-to-end privacy for different levels of centralities for mobile ad hoc local networks, we investigate a range of scenarios where the local ad hoc nodes have low, medium, and high centrality in the face of varying levels of cellular infrastructure surveillance. In offline analysis, we ordered the nodes' degree centralities and choose top 33% as high central nodes and medium (33–66%) as medium centrality and low centrality (below 33%). Due to the sparse connectivity of UNICAL dataset with peak degree connectivity of 6, these centralities result in 2 top ranked, 2 medium ranked, and 2 bottom ranked nodes. Figure 15 shows that, for all levels of connectivity degrees of the local ad hoc nodes, the achieved end-to-end privacy levels for CogPriv are significantly higher than those when cellular network is utilised. CogPriv performs more than 40% better compared to local ad hoc communications for all centrality levels.

In order to show how CogPriv approach adapts to different requirements for privacy, we have performed experiments



(a)

(b)

(c)

Figure 13: End-to-end privacy.

with different traffic types ranging from highly personal through intermediary and not personal types. We assign different privacy requirements to each bundle at the source. At each forwarding decision-making point, CogPriv nodes compare the bundle privacy requirement against the probability of leakage in a network that CogPriv returns. Bundles that have lower privacy requirements than the probability of leakage in a network can be sent via that network. Otherwise, the bundles will be sent via another network or stored at the node if no network meets the bundle privacy requirements. In Section 3, we explain that for bundles which are urgent, the bundles can be sent via cellular network if no trusted

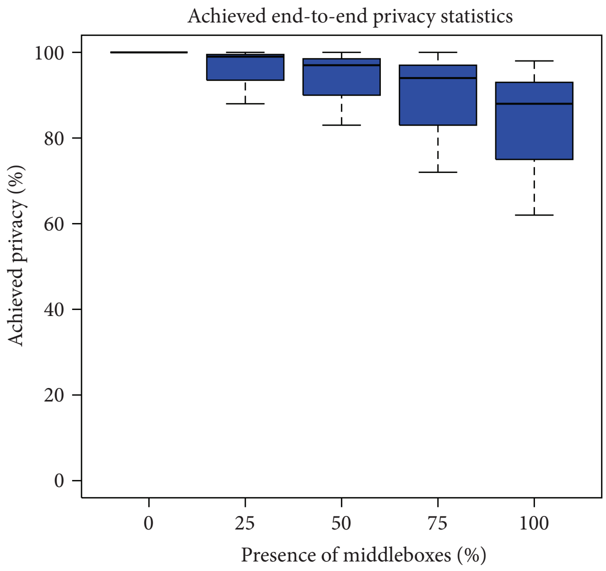


Figure 14: End-to-end privacy statistics.

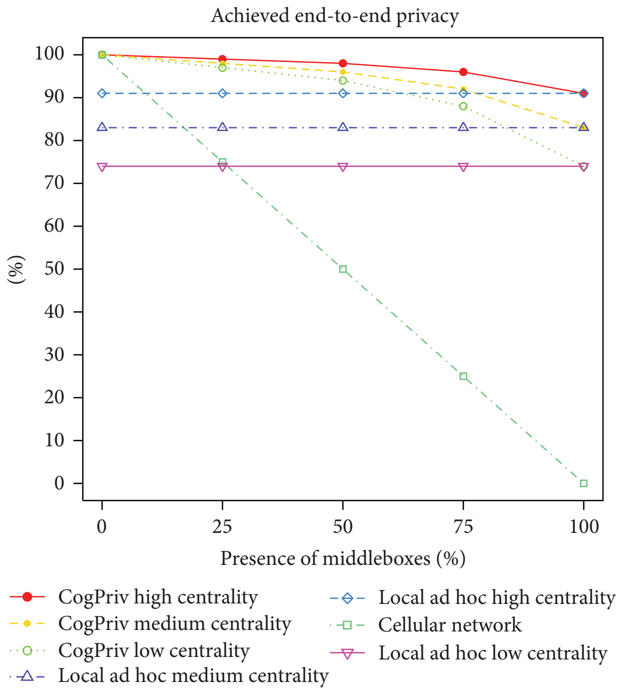


Figure 15: Security with varying centrality of the destination.

local ad hoc route is found within a predetermined timeout period suitable for that bundle which is determined at the application level. Figure 16 shows that Cognitive Privacy approach manages to keep above 98% of achieved end-to-end privacy for medium personal traffic while it keeps above 92% for medium to high privacy traffic. For highly personal traffic, Cognitive Privacy manages to keep above 82% for all levels of middle boxes presence in the cellular network. As expected, we show that the higher the node centralities are, the higher the achieved end-to-end privacy levels are

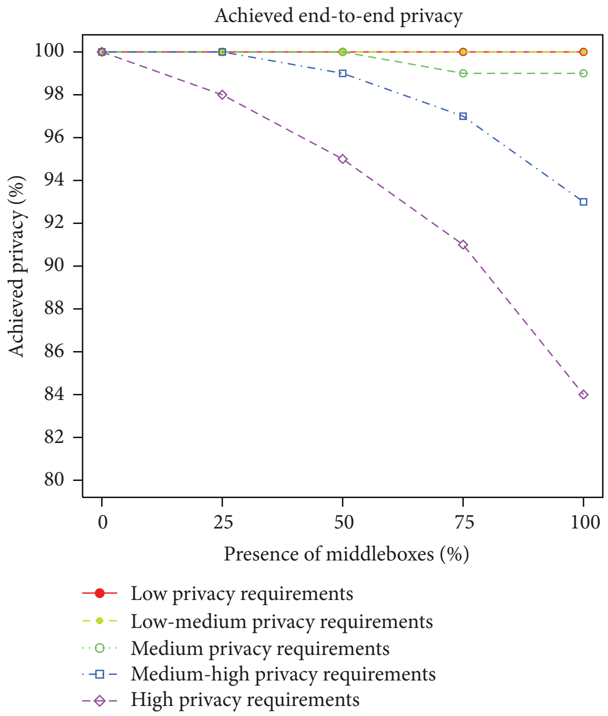


Figure 16: Security with varying privacy requirements.

for all protocols. It is important to observe that the achieved end-to-end privacy levels for CogPriv are above 90% for all levels of degree centralities for low to medium-high level of middlebox presence in the cellular network. For high levels of middlebox presence in the cellular network and for high node centralities, the archived end-to-end privacy for CogPriv is still very high (96%). For medium and low node connectivity, CogPriv manages privacy of around 85% and 75%, respectively, in the face of high levels of middlebox presence in the cellular network. This is very important as it shows that even in both cases when the cellular network is highly compromised and the trusted local ad hoc network is very disconnected and sparse, CogPriv can keep high levels of privacy which converge to the performance of local ad hoc approach that utilises social network structure for forwarding.

5.2.2. End-to-End Delays and Retentiveness Analysis. Figure 17 shows that CogPriv end-to-end delays increase slowly until the infrastructure is fully compromised at which point the delays become the same as they are for the local ad hoc approach. The cellular network approach has the lowest delays but this is due to privacy being compromised and the traffic taking single hop (direct) cellular link between the end nodes.

Figure 18 shows delay distributions for highly private traffic bundles when the cellular infrastructure contains dramatically different amount of middleboxes. We observe that the delays are the lowest when the infrastructure is not compromised as the CogPriv approach takes cellular single hop router to the destination. As CogPriv discovers

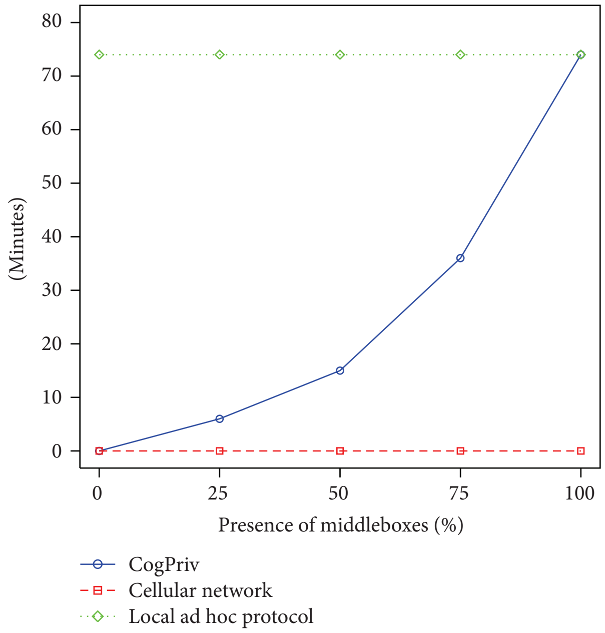


Figure 17: End-to-end delays.

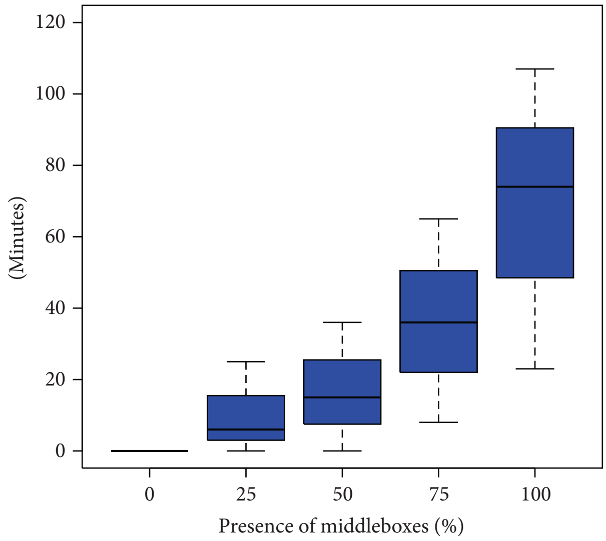


Figure 18: End-to-end delay statistics.

increasing number of middleboxes in the cellular networks, the delays increase but are significantly lower than the local ad hoc approach. Even though there are some bundles that may take up to 25 minutes until 50% of surveillance of the cellular network, the average still remains low and below 17 minutes. For the cellular network where there is 75% to 100% of middlebox presence, the delays range from 10 minutes (min) to 100 minutes (max) and from 3 minute to 75 minutes (average). These sorts of delays are appropriate for nonemergency applications where the users value their privacy and can tolerate delays such as regular daily checks for users with long-term medical conditions.

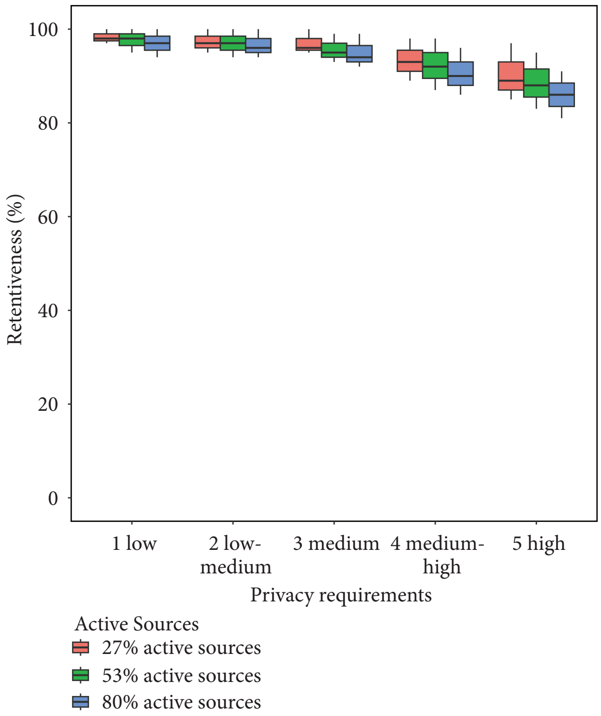


Figure 19: Retentiveness.

Figure 19 shows that CogPriv manages to maintain high levels of retentiveness (available storage) which is 85% for all levels of privacy requirements and for increasing number of active sources. It is important to investigate influence of different levels of privacy requirements as retentiveness gets measured only in ad hoc local forwarding (not cellular). More specifically, as privacy requirements increase and the more CogPriv chooses local forwarding over cellular forwarding which has middleboxes, we show that CogPriv does not significantly decrease available storage. Moreover, even for significant increase of active sources from 27% to 80%, the decrease in retentiveness is only around 1%. This is due to CogPriv utilising effective heuristics on congestion awareness and social graph analytics to predict the best next hop (the heuristic is described in Section 4). It is important to note that for the highest privacy requirements CogPriv will behave as local ad hoc protocol as it will always use only local ad hoc communications and not the cellular network infrastructure.

5.2.3. End-to-End Forwarding Hop Count and Transition Analysis. It is interesting to see in Figure 20 that CogPriv approach does not add additional number of hops compared to local ad hoc communication. We observe that end-to-end number of hops increases as the cellular network privacy decreases but remains lower than it is for local ad hoc forwarding. This is because CogPriv can effectively utilise an opportunity for middlebox-free cellular network whenever possible which allows it to connect to the destination via a single hop. This means that CogPriv does not add to delays compared to the local ad hoc approach while it increases the delays only when the cellular network significantly compromises user privacy.

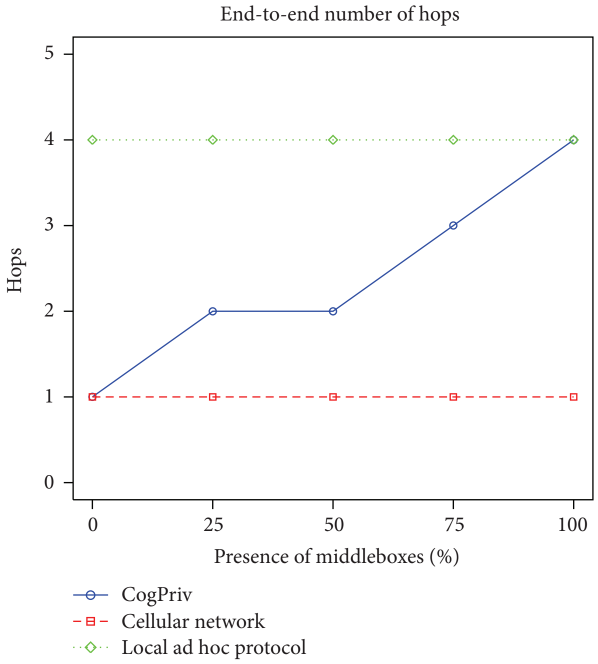


Figure 20: Number of hops.

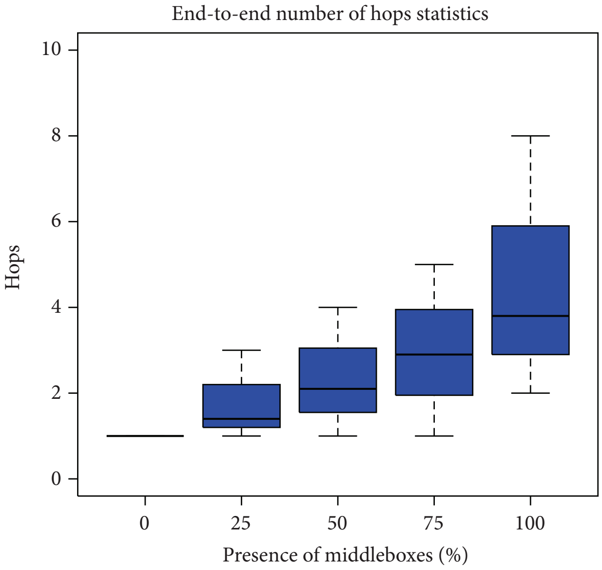


Figure 21: Number of hops statistics.

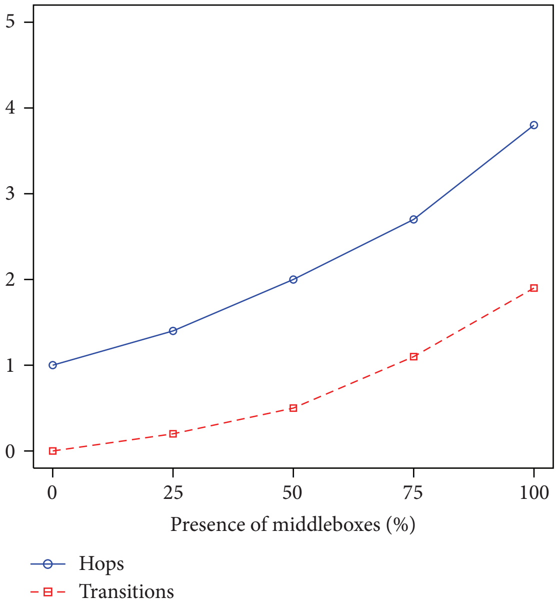


Figure 22: End-to-end number of transitions.

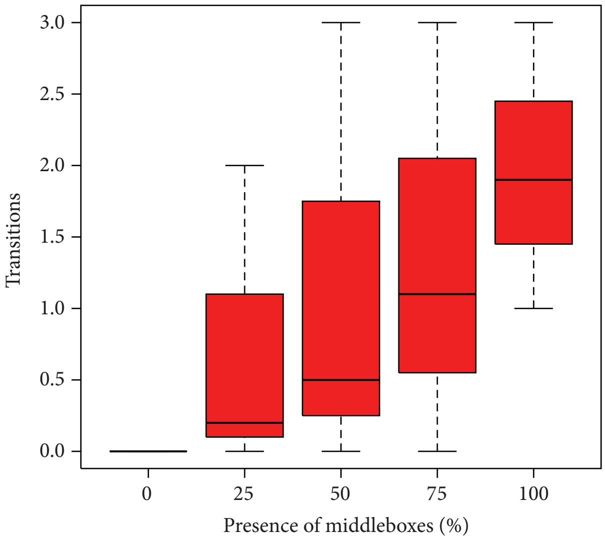


Figure 23: End-to-end transitions statistics.

Figure 21 shows statistical analyses of CogPriv number of hops with increased number of middleboxes in the cellular architecture. We observe that the numbers range between 1 and 4 across all levels of middleboxes presence.

In Figure 22, we show the number of transitions between infrastructure and local ad hoc protocol when the security of the cellular network decreases. It is interesting to see that while the number of hops is relatively low (reaching 4 for highly compromised cellular networks), up to 50% of these hops are transitions between the infrastructure and local communication. This shows that supporting adaptive transitioning between infrastructure and local communication is highly beneficial.

Figure 23 shows that the CogPriv approach keeps the average level of transitions below 2 for all levels of cellular network surveillance but occasionally peaks to 3 for high level of middleboxes in the network. This shows that CogPriv approach adapts well to the presence of middleboxes in the cellular networks while effectively utilising local communication to keep the end-to-end quality of service as high as possible.

The previous figures have shown that delays and hop by hop counts increase as CogPriv moves adaptively from fully

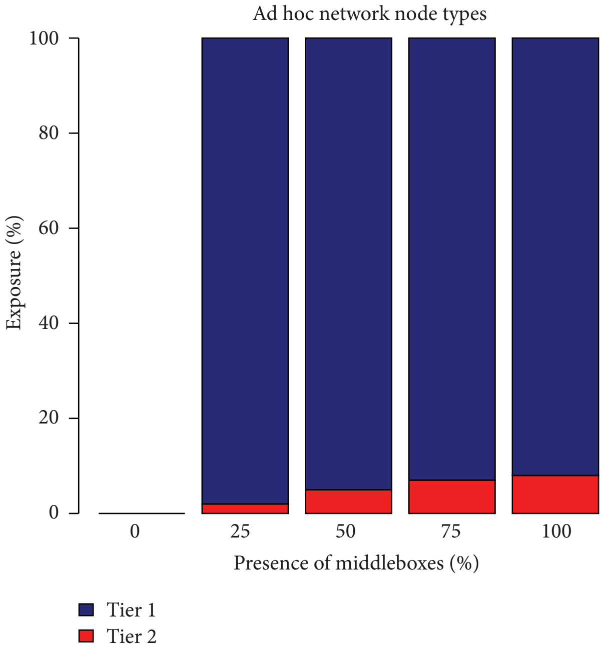


FIGURE 24: Exposure for increasing presence of middleboxes.

cellular mode to the fully opportunistic mode while managing very high levels of end-to-end privacy. More specifically, we show that the CogPriv achieves privacy of end-to-end connections which is almost constant while neither the delays nor the hop count is significantly increased.

5.2.4. Exposure Analysis. We are particularly interested in the issues of privacy being affected negatively despite the fact that no access control was violated. Emerging research shows that users of social media and remote health care applications increasingly prefer to have more control on who sees their data even among the users who are allowed to see their data via user access control rules. For example, while users may be happy that several closest friends of theirs can see and forward their data, they may not be happy that the other friends see some other data (e.g., social versus health related). Even in case of healthcare context, it has been argued that allowing local data control and privileges should be increasingly supported in addition to the central basic services. In this respect, more context sensitive policies can be enforced throughout the distributed communication cloud architecture.

Figure 24 shows percentage of data being exposed to the second tier of friends (those that are not the most trusted but who can still view the content) for increasing percentage of middleboxes in the cellular network. We observe that when percentage of middleboxes is lower than 25%, end-to-end traffic is not exposed to any second-tier friends. For increasing percentage of cellular network spying, we can see the increased reliance on all friends (both first- and second-tier) ranging from 1% to 7%. This is a very low exposure that shows the importance of local context driven data management.

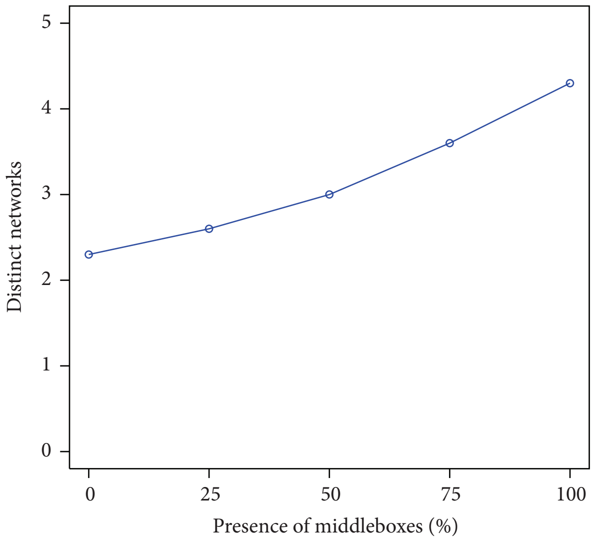


FIGURE 25: Exposure in end-to-end distinct cellular networks.

Related research in social networks has shown that users consider their privacy violated when more different pieces of their data can be linked [39]. Towards this end, our proposal for adaptive privacy-aware forwarding is beneficial as it minimises multiple separate pieces of user data to be viewed, stored, and forwarded by the same node.

In Figure 25, we show the number of distinct networks on end-to-end routes that CongPriv takes for increasing levels of middlebox presence in the infrastructure. For medium to high level of privacy leakage in the cellular infrastructure, CogPriv utilises up to 4 distinct mobile networks and thus prevents the same compromised network provider from accessing and gathering different pieces of information about the user. For example, if we assume that a bundle gets forwarded via three mobile privacy providers with 25% privacy leakage, this does not add up to a total of 75% privacy leakage but remains in the low 25%.

6. Conclusions and Future Work

We proposed Cognitive Privacy (CogPriv) framework as an integral and core part of future Personal Clouds and pervasive communications. At the core of our proposal is the idea that, in mobile social world, privacy raises new challenges that go beyond typical binary allowed/forbidden access control and should take the form of cooperative, collaborative, and context dependent stochastic distributed decision-making. We argue that this new type of privacy can be called "Cognitive Privacy" as it on-the-fly senses and adapts to the infrastructure behaviour, strength/frequency of (mobile) social ties, and/or reputation of other nodes/people. Therefore, for different types of data and user context, the user may prefer to negotiate different levels of privacy.

We showed that CogPriv preserves end-to-end privacy levels to a high level across different network topologies and cellular network ad hoc middlebox distributions as well as different traffic types. As our future work, we plan to deploy CogPriv and Personal Clouds in real-world scenarios in collaboration with Nottingham CityCare Partnership's initiatives to build healthier communities and improving long-term health and wellbeing of local people [40]. We plan to design new user-friendly interfaces that would improve usability of Personal Clouds particularly in respect of providing real time feedback to the user on the levels of privacy of their data. More specifically, we argue that it would be beneficial to allow users to disrupt some decisions of CogPriv at certain circumstances such as changed level of urgency, for example, when the user may prefer to wait longer and maintain higher level of privacy versus delivering the data to the destinations.

Competing Interests

The author declares that she has no competing interests.

References

[1] N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, N. Weaver, and V. Paxson, "Beyond the radio: illuminating the higher layers of mobile networks," in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '15)*, pp. 375–387, ACM, Florence, Italy, May 2015.

[2] M. Radenkovic and N. Milic-Frayling, "Demo: RasPiPCloud: a light-weight mobile personal cloud," in *Proceedings of the 10th ACM MobiCom Workshop on Challenged Networks (CHANTS '15)*, pp. 57–58, Paris, France, September 2015.

[3] A. Y. Ding, J. Crowcroft, and S. Tarkoma, "Poster: SoftOffload: a programmable approach toward collaborative mobile traffic offloading," in *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '14)*, p. 368, Bretton Woods, NH, USA, June 2014.

[4] LXC—Linux Containers, https://linuxcontainers.org/.

[5] N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, and V. Paxson, "Header enrichment or ISP enrichment?: emerging privacy threats," in *Proceedings of the ACM SIGCOMM Workshop on Hot Topics in Middleboxes and Network Function Virtualization (HotMiddlebox '15)*, pp. 25–30, London, UK, August 2015.

[6] A. Y. Ding, B. Han, Y. Xiao et al., "Enabling energy-aware collaborative mobile data offloading for smartphones," in *Proceedings of the 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '13)*, New Orleans, Lo, USA, June 2013.

[7] A. Balasubramanian, R. Mahajan, and A. Venkataramani, "Augmenting mobile 3G using WiFi," in *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services (MobiSys '10)*, pp. 209–222, San Francisco, Calif, USA, June 2010.

[8] K. Lee, J. Lee, Y. Yi, I. Rhee, and S. Chong, "Mobile data offloading: how much can WiFi deliver?" in *Proceedings of the 6th International COnference (Co-NEXT '10)*, Philadelphia , Pa, USA, 2010.

[9] A. Y. Ding, B. Han, Y. Xiao et al., "Enabling energy-aware collaborative mobile data offloading for smartphones," in *Proceedings of the 10th Annual IEEE Communications Society Conference on Sensing and Communication in Wireless Networks (SECON '13)*, pp. 487–495, New Orleans, La, USA, June 2013.

[10] N. Ristanovic, J.-Y. Le Boudec, A. Chaintreau, and V. Erramilli, "Energy efficient offloading of 3G networks," in *Proceedings of the 8th International Conference on Mobile Ad-hoc and Sensor Systems (MASS '11)*, pp. 202–211, IEEE, Valencia, Spain, October 2011.

[11] X. Zhuo, W. Gao, G. Cao, and Y. Dai, "Win-coupon: an incentive framework for 3G traffic offloading," in *Proceedings of the 19th IEEE International Conference on Network Protocols (ICNP '11)*, pp. 206–215, Vancouver, Canada, October 2011.

[12] E. Bulut and B. K. Szymanski, "WiFi access point deployment for efficient mobile data offloading," in *Proceedings of the 1st ACM International Workshop on Practical Issues and Applications in Next Generation Wireless Networks (PINGEN '12)*, pp. 45–50, ACM, Istanbul , Turkey, August 2012.

[13] J. Korhonen, T. Savolainen, A. Ding, and M. Kojo, "Toward network controlled IP traffic offloading," *IEEE Communications Magazine*, vol. 51, no. 3, pp. 96–102, 2013.

[14] S. Liu and A. Striegel, "Casting doubts on the viability of WiFi offloading," in *Proceedings of the ACM SIGCOMM Workshop on Cellular Networks: Operations, Challenges, and Future Design (CellNet '12)*, pp. 25–30, Helsinki, Finland, August 2012.

[15] E. Romero, J. Blesa, A. Tena, G. Jara, J. Domingo, and A. Araujo, "Cognitive test-bed for wireless sensor networks," in *Proceedings of the IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN '14)*, pp. 346–349, McLean, Va, USA, April 2014.

[16] A. Razaghpanah, N. Vallina-Rodriguez, S. Sundaresan et al., "Haystack: in situ mobile traffic analysis in user space," http://arxiv.org/abs/1510.01419.

[17] E. Shi, T.-H. H. Chan, E. G. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proceedings of the Network and Distributed System Security (NDSS '11)*, August 2011.

[18] M. Joye and B. Libert, "A scalable scheme for privacy-preserving aggregation of time-series data," in *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1–5, 2013, Revised Selected Papers*, vol. 7859 of *Lecture Notes in Computer Science*, pp. 111–125, Springer, Berlin, Germany, 2013.

[19] K. Leontiadis, R. Elkhiyaoui, and R. Molva, "Private and dynamic time-series data aggregation with trust relaxation," in *Cryptology and Network Security*, D. Gritzalis, A. Kiayias, and I. Askoxylakis, Eds., vol. 8813 of *Lecture Notes in Computer Science*, pp. 305–320, 2014.

[20] M. Radenkovic and I. Vaghi, "Adaptive user anonymity for mobile opportunistic networks," in *Proceedings of the 7th ACM International Workshop on Challenged Networks*, pp. 79–81, ACM, August 2012.

[21] A. Grundy and M. Radenkovic, "Promoting congestion control in opportunistic networks," in *Proceedings of the 6th Annual IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '10)*, pp. 324–330, Niagara Falls, Canada, October 2010.

[22] M. Radenkovic, A. Benslimane, and D. McAuley, "Reputation aware obfuscation for mobile opportunistic networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 1, pp. 230–240, 2015.

[23] H. Haddadi, H. Howard, A. Chaudhry, J. Crowcroft, A. Madhavapeddy, and R. Mortier, "Personal data: thinking inside the box," http://arxiv.org/abs/1501.04737.

[24] M. Y. Mun, D. H. Kim, K. Shilton, D. Estrin, M. Hansen, and R. Govindan, "PDVLoc: a personal data vault for controlled

location data sharing," *ACM Transactions on Sensor Networks*, vol. 10, no. 4, article 58, 2014.

[25] K. Scott and S. Burleigh, "Bundle protocol specification," RFC 5050, 2007.

[26] IBR-DTN, https://trac.ibr.cs.tu-bs.de/project-cm-2012-ibrdtn.

[27] S. Schildt, T. Lorentzen, J. Morgenroth, W.-B. Pöttner, and L. Wolf, "Free-riding the bittorrent DHT to improve DTN connectivity," in *Proceedings of the 7th ACM International Workshop on Challenged Networks (CHANTS '12)*, pp. 9–15, ACM, Istanbul, Turkey, August 2012.

[28] M. Radenkovic and A. Grundy, "Efficient and adaptive congestion control for heterogeneous delay-tolerant networks," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1322–1345, 2012.

[29] M. Radenkovic and A. Grundy, "Framework for utility driven congestion control in delay tolerant opportunistic networks," in *Proceedings of the 7th International Wireless Communications and Mobile Computing Conference (IWCMC '11)*, pp. 448–454, Istanbul, Turkey, July 2011.

[30] M. Radenkovic and A. Grundy, "Congestion aware data dissemination in social opportunistic networks," *Mobile Computing and Communications Review*, vol. 14, no. 3, pp. 31–33, 2010.

[31] M. Radenkovic and A. Grundy, "Congestion aware forwarding in delay tolerant and social opportunistic networks," in *Proceedings of the 8th International Conference on Wireless On-Demand Network Systems and Services (WONS '11)*, pp. 60–67, Bardonecchia, Italy, January 2011.

[32] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '03)*, pp. 27–34, ACM, New York, NY, USA, 2003.

[33] M. Mondal, Y. Liu, B. Viswanath, K. P. Gummadi, and A. Mislove, "Understanding and specifying social access control lists," in *Proceedings of the 10th Symposium on Usable Security and Privacy (SOUPS '14)*, Menlo Park, Calif, USA, July 2014.

[34] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant MANETs," *IEEE Transactions on Mobile Computing*, vol. 8, no. 5, pp. 606–621, 2009.

[35] A. Socievole, F. De Rango, and A. Caputo, "Wireless contacts, Facebook friendships and interests: analysis of a multi-layer social network in an academic environment," in *Proceedings of the IFIP Wireless Days (WD '14)*, pp. 1–7, Rio de Janeiro, Brazil, November 2014.

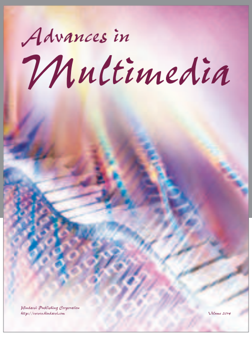
[36] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proceedings of the 2nd International Conference on Simulation Tools and Techniques (Simutools '09)*, article 55, p. 10, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, Belgium, 2009.

[37] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau, *CRAWDAD Dataset Cambridge/Haggle (v. 20090529)*, 2009.

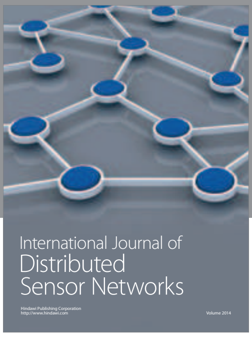
[38] F. Benbadis and J. Leguay, "CRAWDAD dataset upmc/rollernet (v. 20090202)," February 2009, http://crawdad.org/upmc/rollernet/20090202.

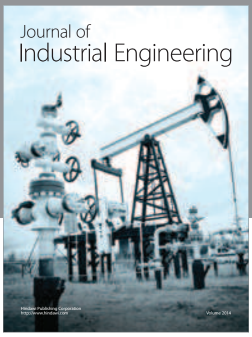
[39] M. Mondal, P. Druschel, K. P. Gummadi, and A. Mislove, "Beyond access control: managing online privacy via exposure," in *Proceedings of the Workshop on Usable Security*, 2014.

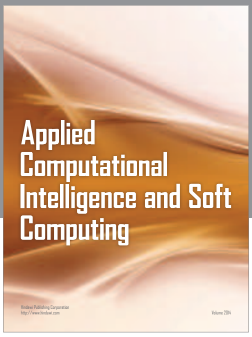
[40] Nottingham CityCare Partnership, http://www.nottinghamcitycare.nhs.uk/.

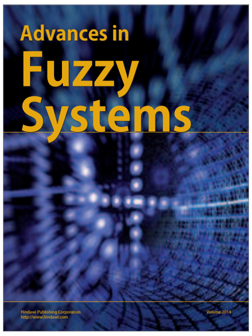

Advances in
Multimedia

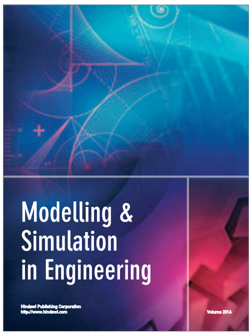
The Scientific
World Journal

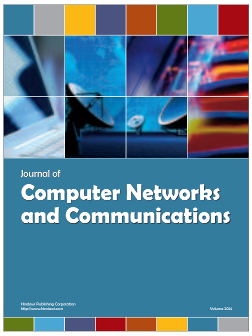

International Journal of
Distributed
Sensor Networks

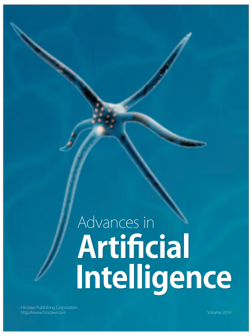

Journal of
Industrial Engineering

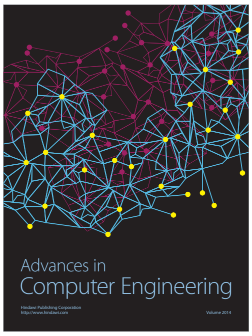

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

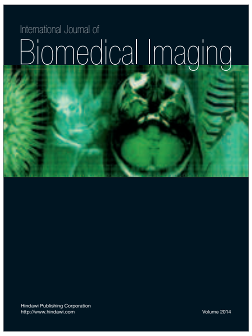

Modelling &
Simulation
in Engineering

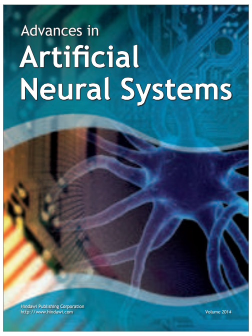

Journal of
Computer Networks
and Communications

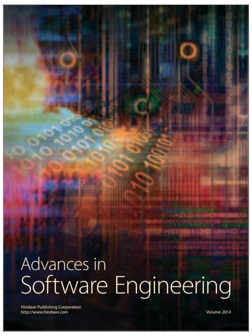

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

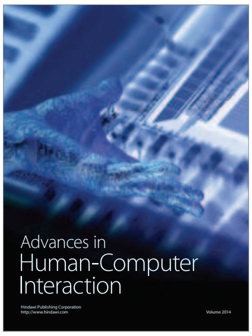
International Journal of
Computer Games
Technology

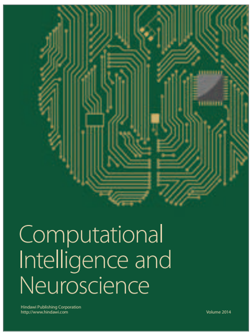

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering