A Privacy-Level Model of User-Centric Cyber-Physical Systems

Nikolaos E. Petroulakis[1], Ioannis G. Askoxylakis[1], Apostolos Traganitis[1], and George Spanoudakis[2]

[1] Institute of Computer Science, Foundation for Research and Technology - Hellas, Heraklion, Greece
{npetro,asko,tragani}@ics.forth.gr
[2] School of Informatics, City University London, London, UK
g.e.spanoudakis@city.ac.uk

Abstract. In an interconnected cyber-world, Cyber-Physical Systems (CPSs) appear to play an increasingly important role in smart ecosystems. A variety of resource-constrained thin clients, such as sensors, RFIDs, actuators and smart devices, are included in the list of CPS. These devices can be used in a number of medical, vehicular, aviation, military and smart cities applications. A plethora of sensitive data is transmitted in insecure wireless or wired environments whilst adversaries are eager to eavesdrop, modify or destroy sensed data invading the privacy of user-centric CPSs. This work presents an overview and analysis of the most effective attacks, privacy challenges and mitigation techniques for preserving the privacy of users and their interconnected devices. In order to preserve privacy, a privacy-level model is proposed in which users have the capability of assigning different privacy levels based on the variety and severity of privacy challenges and devices' capabilities. Finally, we evaluate the performance of specific CPSs at different privacy-levels in terms of time and consumed energy in an experimental test-bed that we have developed.

Keywords: Privacy, Privacy-level model, Security, Cyber-Physical Systems.

1 Introduction

Cyber-Physical System (CPS) is a term used to describe integrations of computation, networking and physical processes [1]. These embedded computers and networks may monitor and control devices that are taking measurements from sensors or RFIDs. One of the most important issues of embedded systems is the small amount of theoretical work to describe how to design computer-based control systems and the work in [2] addresses this problem. Although CPS and the Internet of Things (IoT) both aim to increase the interconnection of constrained devices in cyber-space and the physical world, the term CPS is commonly used in the USA and the National Science Foundation (NFS) [3] while the European Commission refers IoT in a variety of FP7 Calls [4]. The most important

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 338–347, 2013.

difference is that the main target of IoT is to develop an open platform and infrastructure for communication between smart objects such as sensors whereas CPS focuses on the exchange and feedback of information in order to control devices in the physical world [5].

CPS are small ubiquitous devices, such as sensors, actuators, RFID tags, smart phones and embedded systems able to interact and interconnect with physical elements. They can be used to vehicular networks, medical systems, the aviation industry, defense, environmental monitoring, entertainment, robotic manufacturing, electricity generation and distribution, etc. [1]. They can be categorized into three categories: monitor and detection, process and evaluation, actuation and prevention. An extensive preview of CPS in the aerospace industry perspective is presented by Boeing in [6]. They have declared that CPS investments should include industry-critical mass and multiple technology domains to acquire the required results. Authors in [7] present a human factor-aware service scheduling in vehicular CPS that depends on how drivers could benefit from such systems. Security and privacy in smart ecosystems are both critical for public safety. The large development of interconnected cities, in which humans and devices interact, generates large-scale security threats, especially for public security. CPS face many privacy challenges because of the requirements for real-time interaction and the lack of appropriate physical security due to geographical dispersion [8] and the limited resources and capabilities of thin clients.

In this paper, we extend our previous work in [9–11] by investigating attacks, challenges and methods to preserve privacy in user-centric thin clients such as CPSs. We analyze the most severe privacy challenges occurred from passive attacks, such as eavesdropping and traffic analysis, and from active attacks, such as impersonation and jamming. Suitable countermeasures are described to protect data and identity, location and routing paths. To define the privacy-level model, we group the described mitigation mechanisms into three categories according to the utilized parameters: standard parameters, fake parameters and changing parameters. Based on these categories a privacy-level model is proposed, consisting of three different levels of privacy corresponding to different privacy challenges and attacks. This model can be applied in a variety of CPSs independently of device's capabilities and operating systems. Furthermore, the privacy-level model developed here is evaluated in an experimental test-bed.

The remainder of this paper is organized as follows. In section 2, we describe the most critical attacks and privacy threats whilst in section 3, we construct the privacy-level model to mitigate the previously described privacy threats. In Section 4, we evaluate the privacy-level model using an experimental setup evaluating the trade-off between privacy and energy. Finally, we conclude this paper in Section 5.

2 Privacy Challenges and Attacks on CPSs

The massive production and transfer of sensitive data exposes the danger of privacy violation in user-centric CPSs. The vast amount of transmitted data from

devices such as sensors, RFID and embedded systems, may reveal information about location and routing paths or other sensitive details such as private data and identities. CPSs are usually located in uncontrolled environments where physical attacks might occur [12]. Furthermore, their limited ability to securely store key fingerprints, their tiny computation capabilities and their limitations in power and energy make them vulnerable to adversaries. Security and privacy attacks include physical and cyber tampering or compromising devices. In the following approach we concentrate mainly on passive or active attacks that invade the privacy of user-centric CPSs.

2.1 Passive Attacks

Passive are the attacks in which an adversary monitors traffic without interacting with the victim or modifying transmitted data. The most common passive attacks are eavesdropping and traffic analysis. Eavesdropping occurs when an adversary monitors and listens to the exchanged data with the intention to extract private data. The disclosure of sensitive information such as identities and message payload, are severe privacy violations from eavesdropping. For example, the disclosure of sensed medical data such as patient's personal data, blood pressure, vital signs or sugar level, transmitted to a remote hospital or to a doctor's office, may reveal the patient's identity and condition. On the other hand, traffic analysis attacks can be applied by adversaries who do not have the ability to decrypt data payload, but they can obtain private information such as data sources, the location of devices and data routes, by the use of sniffers and packet analyzers on the wireless data transmission for tracking the traffic flow information hop-by-hop [12]. The problem of the panda and the hunter describes the situation in which scientists attempt to locate the position of a panda but they have to hide its location from panda hunters as well [13]. Revealing the topology, nature and routing paths of a transmission could be used by adversaries to track, destroy interrupt and invade the privacy of a CPS. Moreover, the danger of a compromised relay node is a result of location disclosure.

2.2 Active Attacks

An active attack occurs when an adversary attempts to modify exchanged messages, destroy the communication or replay transmitted data. The most severe active attacks which invade the privacy of CPSs are impersonation and denial of service. Impersonation attacks involve the interaction of an adversary with the human user. The adversary acts either as a man in the middle or as a masquerade, pretending to be a legal node in the network to apply spoofing attacks. These kinds of attacks appear to be not only critical for a user's privacy but also the consequences of such attacks could be extremely dangerous. For instance, an impersonation attack on a CPS, interconnected with a patient, may cause false alarms to doctor's office. And the modification of medical data can put patient's life in danger. Denial of Service (DoS) can characterize any kind of attack, which attempts to make the network resources unavailable. An active

adversary applies DoS attacks by destroying or modifying the communication channel. The preservation of privacy is disrupted when an attacker applies collisions or jamming attacks creating electromagnetic interference. The lack of channel availability has a severe influence on the privacy of CPS. An adversary, causing interference in a channel in which users interchange sensitive or critical messages, may cause reportable privacy violations, such as data destruction or infinite retransmission of messages, exhausting the batteries of resource constrained CPS. Furthermore, the delayed transmission of critical information, such as private medical data of a patient to the doctors database, means the patients safety might be endangered.

3 The Privacy-Level Model

In this section, we define a privacy-level model based on the aforementioned attacks and challenges to preserve privacy in CPS. Other works, such as [14–16], focus on location privacy and route protection, providing partial privacy protection. Authors in [17] propose a full network and level privacy solution for WSN consisting of three schemes. In the first scheme, anonymity of source node's identity and location assures that path will reach their destination through trusted intermediate nodes. Forwarding packets from multiple secure paths is described in the second scheme. Finally, data secrecy and packet authentication in the presence of identity anonymity is proposed in the third scheme.

In our approach, we present a privacy-level model combining different privacy countermeasures for mitigating critical privacy dangers and attacks as described in the previous section. The main concept of this approach is that a user will be able to assign the suitable privacy level of a network, consisting of CPSs, depending on the security challenges and privacy risks. And as the level is increased we assume the protection becomes stronger. The advantage of our privacy model is that we use generic countermeasures, which can applied in a variety of CPS running different operation systems and having different capabilities. To construct the privacy-level model, we group in one model effective mitigation mechanisms to protect identity, data, routing paths and location protection. Based on our research, we can categorize countermeasures into three categories. The first category includes standard privacy countermeasures, such as encryption. In the second category, fake parameters, such as dummy data and fake paths, are assigned to protect data transmission from adversaries. Finally, the last category includes countermeasures which change frequently such as multi-paths and frequency hopping. More precisely, the three privacy-levels are described as follows.

3.1 Level 1 - Standard Parameters

In the first level, standard parameters have been assigned to mitigate attacks. When cryptographic algorithms are not used, an attacker can compromise the transmitted data easily. In order to protect the payload of transmitted data, encryption mechanisms should be used for encrypting data and prevent adversaries from passive listening and data falsification. To protect the identity of

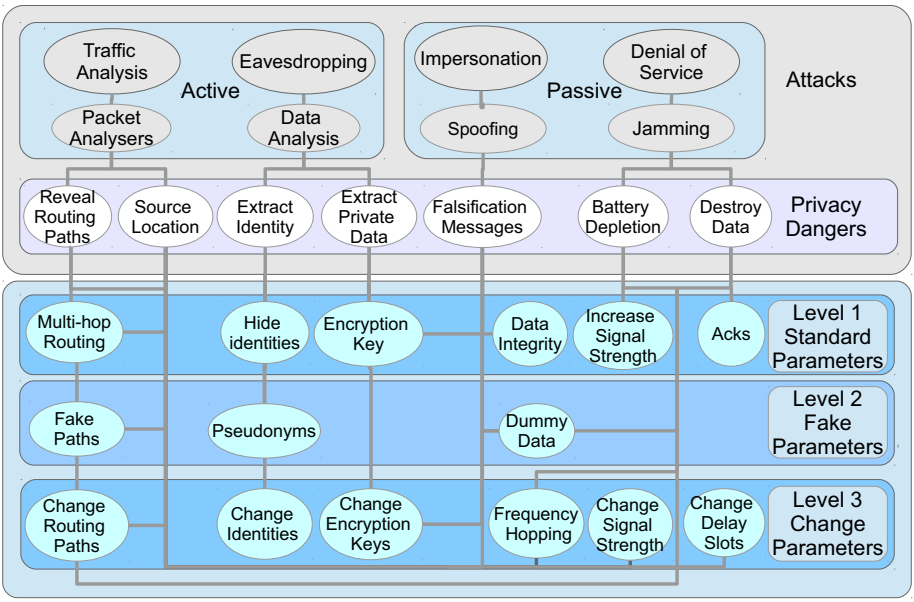

Fig. 1. The Privacy-level Model

CPS, identities of messages should be hidden either encrypted or not being assigned [17]. Furthermore, if a packet has reached the range of radio waves then it is difficult to locate the source [18]. This can be applied by the use of multi-hop routing which can also prevent adversaries from identifying the source and the routing paths of transmissions. Data integrity confirms that data has not been modified. Integrity is achieved by the use of Message Integrity Codes (MICs) or Message Authentication Codes (MACs). Furthermore, the increase of signal strength could mitigate weak jamming attacks [19]. Even though acknowledgment mechanisms do not guarantee data integrity, the use of them can ensure valid packet reception.

3.2 Level 2 - Fake Parameters

The second privacy level is defined by using fake parameters. Pseudonyms can be an effective way to hide the real identity of a node. Although pseudonyms seem to be an effective solution, fixed pseudonyms cannot prevent adversaries from deducing the topology of the network through traffic analysis [18]. When actual encrypted data are not exchanged, dummy messages can be send to mask the channel, hiding the actual data transmission. This mechanism can keep the bandwidth constant and hide the traffic to confuse passive listeners from effective eavesdropping and traffic analysis [12, 15]. Finally, the creation of fake paths could potentially prevent an adversary from tracking the routing path and destroying the transmission [15, 20].

3.3 Level 3 - Change Parameters

In the third layer, stronger privacy attacks can be prevented by changing parameters frequently. As described in the first level, encryption can be an effective way to protect data. However, an adversary knowing the password may decrypt ciphered data. To avoid the danger of revealing the encryption key, a predefined set of anonymous keys changing frequently could protect the encrypted transmission between CPS. Furthermore, changing identities frequently may thwart attackers from identity disclosure. The received signal strength and the time interval appear to be one of the most major factors in locating the position of a CPS [21]. Therefore, the signal strength and the time interval of the transmission should be changed frequently. Thus, random delay slots can used for collision avoidance. Frequency hopping can prevent not only continuous impersonation or passive listening attacks but also anomaly and jamming attacks [22], protecting source location and routing paths, and assuring data transmission [19]. Finally, changing routing paths may thwart adversaries from jamming attacks [14]. In Figure 1 we depict the proposed privacy-level model corresponding to the described attacks, privacy challenges and suitable countermeasures.

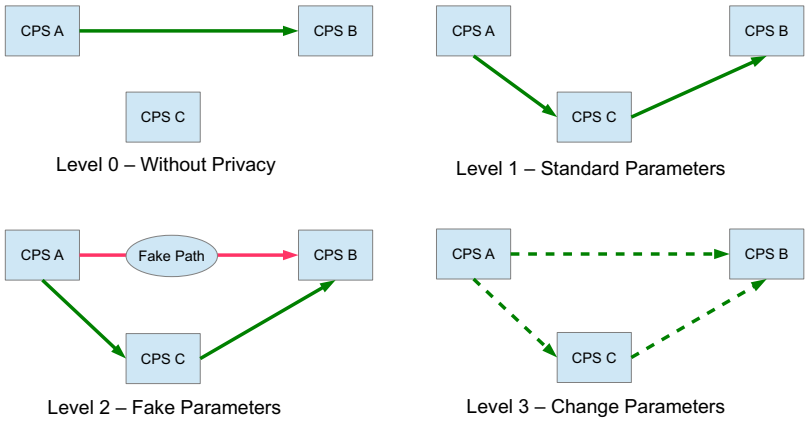

Fig. 2. Topology of the Privacy-level Scenarios

4 Evaluation of the Privacy-Level Model

In this section, we evaluate the proposed privacy-level model investigating the trade-off between energy consumption and privacy protection of each privacy level. The energy needed for computation of each level will increase along with the increase of the security level. Moreover, the time needed to execute some of the more time-consuming procedures, affects the consumed energy as well. The topology of the model consists of three nodes, CPS A, CPS B and CPS C. CPS A acts as the transmitter and CPS B acts as the receiver. The main target of

CPS A is to send a specific number of packets to CPS B. CPS C acts as a relay node to forward transmitted messages from CPS A to CPS B when multi-hop routing is applied. In Figure 2, we depict the topology of the applied scenarios based on the three described privacy levels and level zero which is assigned when privacy protection is not required or not applied.

4.1 Test-Bed Setup

To investigate the energy consumption of the different levels of privacy model, we extend our previously developed test-bed setup [10, 11]. The experimental test-bed consists of three Digi XBee Pro 802.15.4 devices which correspond to CPS A, CPS B and CPS C. All devices are connected through their serial cable with Matlab. Suitable algorithms have been developed in order to evaluate the performance and the consumed energy for each of the described privacy-levels. In the following experiments CPS A sends to CPS B 1000 packets of 100 bytes each. We conduct four different experiments comparing the results of the three privacy levels with level 0, which is the level without any privacy protection. In all four scenarios, we measure the electric current of CPS. To do this, we used a True-RMS polymeter with USB output that enabled us to store the measurements of each experiment in Matlab as well.

4.2 Performance Evaluation

In this part, a description of the conducted experiments is presented. In the first scenario, CPS A sends the specific number of packets to CPS B. Both devices assign similar configuration parameters such as minimum power level and the same channel. In the second scenario, a relay node CPS C is added to forward the traffic from CPS A to CPS B. To avoid weak jamming attacks, the power level of each device is increased at the maximum. Data transmission is assured by the use of acknowledgments, and Maxstream header MAC of XBee sensors enable data integrity. To prevent passive listeners, data privacy is ensured by the use of AES encryption. To protect identity of transmitted messages, we do not assign any identity in their header of messages. In the third scenario, fake data is transmitted in fake paths. Two types of transmissions are applied, a fake and an actual one. In our experiment, CPS A sends 10 actual packets through the relay node CPS C and then 10 fake unencrypted messages directly to CPS B. This procedure is repeated until 1000 actual data are received by CPS B. Finally, in the fourth scenario, parameters are changed frequently. To hide the location of the transmitter, variations in signal strength and in time delay are employed. Frequency hopping is also used to avoid jamming attacks. Multi-path and multi-hop routing is applied to protect the topology of routing paths. To hide the identity of the transmission, CPS A changes its id frequently. Finally, data encryption is assured by the use of a set of predefined encryption keys. The procedure is completed when 1000 messages are received by CPS B.

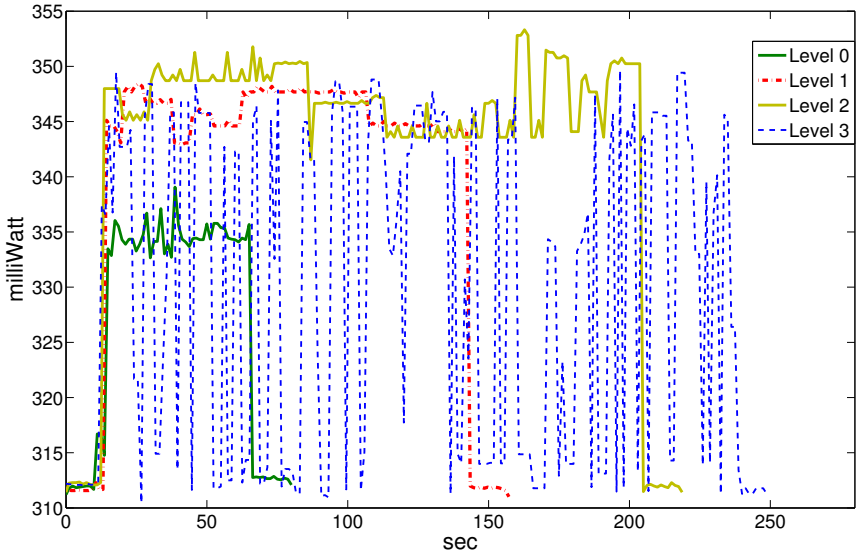

Fig. 3. Energy Consumption of the different Privacy levels

4.3 A Comparison of the Experimental Results

In the last part of this section, we present the results of the conducted experiments. The consumed energy of the experiments, which correspond the four different privacy levels, is depicted in Figure 3. The consumed energy of Level 1 is 142% higher compared to consumed energy of Level 0. This can be explained because of the multi-hop routing, the encryption and the increase of signal strength. In the Level 2, the consumed energy is about 235% higher compared to Level 0 and 46% higher compared to Level 1. The transmission of fake data in Level 2 is the main factor of the increase in consumed energy. The frequent changing parameters affect the needed energy in Level 3. The consumed energy is increased by 297% compared to Level 0, by 64% compared to Level 1 and by 12% compared to Level 2. Finally, a comparison of the consumed energy and time needed of the four different scenarios is presented in Table 1.

The experimental evaluation of the privacy-level model has shown many interesting results. The trade-off between energy and privacy appears to be an important factor for preserving privacy in CPS. The chosen method, measuring the electric current, proved to be an effective way to measure the energy consumption. Single measurements such as monitoring the CPU usage or memory use cannot reflect exactly the total consumed energy of the modules. Therefore, the employed setup was appropriate. This research work has verified our prior assumption concerning the impact on energy consumption in CPS due to different privacy challenges, evaluating the performance of the proposed privacy-level model.

Table 1. Comparison of Needed Time and Energy Consumption

Privacy Level	Time (seconds)	Energy (milliWatt-Hour)
Level 0	50.1	5.35
Level 1	127.8	12.98
Level 2	190.0	18.99
Level 3	224.7	21.29

5 Conclusion

In this paper a privacy-level model of user-centic cyber-physical systems was proposed. The plethora of CPS and their connection with user-centric applications have raised new issues and privacy threats. Privacy challenges appear due to the lack of suitable privacy mechanisms because of the limited resources of CPS. In order to define this privacy model a brief description of a variety of attacks and privacy challenges, was described. The proposed privacy-model applies generic privacy countermeasures which can applied in a number of CPS independently of their capabilities and running operating systems. The main idea is that an operator would be able to assign a specific privacy level based on the privacy challenges of a network. To evaluate this privacy-level model, an experimental investigation of the energy consumption of this privacy-level model in CPS was conducted which indicated that the energy and time needed for computation of each level was increased with the increase of level. The investigation of the trade-off between energy and privacy of each different level completed this work.

References

1. Edward, A.L.: Cyber Physical Systems: Design Challenges. In: 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), pp. 363–369 (May 2008)
2. Wolf, W.: Cyber-physical systems. In: Embedded Computing, pp. 88–89 (2009)
3. Program Solicitation. Cyber-Physical Systems (CPS) Program Solicitation NSF 13-502 Replaces Document (S), pp. 1–13 (2013)
4. Frederixand, F.: D Sector. Internet of Things policy of the European Commission Content IoT Policy IoT in Framework 7 R & D (2010)
5. Ma, H.D.: Internet of things: Objectives and scientific challenges. Journal of Computer Science and Technology 26, 919–924 (2011)
6. Winter, D.: Cyber Physical Systems - An Aerospace Industry Perspective. Boeing, 1–18 (2008)
7. Li, X., Yu, X., Wagh, A., Qiao, C.: Human factors-aware service scheduling in vehicular cyber-physical systems. In: 2011 Proceedings of the INFOCOM, pp. 2174–2182 (April 2011)
8. Neuman, C.: Challenges in security for cyber-physical systems. In: ...Future Directions in Cyber-physical Systems Security (2009)
9. Petroulakis, N.E., Askoxylakis, I., Tryfonas, T.: Life-logging in Smart Environments: Challenges and Security Threats. In: The 2nd IEEE ICC Workshop on Convergence among Heterogeneous Wireless Systems in Future Internet (ConWire), Ottava, Canada (June 2012)

10. Petroulakis, N.E., Tragos, E.Z., Askoxylakis, I.G.: An Experimental Investigation on Energy Consumption for Secure Life-logging in Smart Environments. In: The 17th IEEE International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD), Barcelona, Spain (September 2012)
11. Petroulakis, N.E., Tragos, E.Z., Fragkiadakis, A.G., Spanoudakis, G.: A lightweight framework for secure life-logging in smart environments. In: Elsevier Information Security Technical Report (2012)
12. Li, N., Zhang, N., Das, S.K., Thuraisingham, B.: Privacy preservation in wireless sensor networks: A state-of-the-art survey. Ad Hoc Networks 7(8), 1501–1514 (2009)
13. Ozturk, C., Zhang, Y., Trappe, W.: Source-location privacy in energy-constrained sensor network routing. In: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN 2004, p. 88 (2004)
14. Gruteser, M., Schelle, G., Jain, A.: Privacy-aware location sensor networks. In: Proceedings of the 9th ... (2003)
15. Luo, X., Ji, X., Park, M.-S.: Location Privacy against Traffic Analysis Attacks in Wireless Sensor Networks. In: 2010 International Conference on Information Science and Applications, pp. 1–6 (2010)
16. Kamat, P., Zhang, Y., Trappe, W., Ozturk, C.: Enhancing Source-Location Privacy in Sensor Network Routing. In: 25th IEEE International Conference on Distributed Computing Systems, ICDCS 2005, pp. 599–608 (2005)
17. Shaikh, R.A., Jameel, H., D'Auriol, B.J., Lee, H., Lee, S., Song, Y.-J.: Achieving network level privacy in Wireless Sensor Networks. Sensors (Basel, Switzerland) 10(3), 1447–1472 (2010)
18. Veeranna, M., Krishna, V.R., Jamuna, D.: Enhancement of Privacy Level in Wireless Sensor Network. ijecse.com 1, 1024–1029 (2012)
19. Xing, K., Sundhar, S., Srinivasan, R., Rivera, M.: Attacks and Countermeasures in Sensor Networks: A Survey A wireless sensor network (WSN) is comprised of a large number of sensors that, pp. 1–28 (2005)
20. Sen, J.: A Survey on Wireless Sensor Network Security. International Journal of Communication Networks and Information Security (IJCNIS) 1(2), 55–78 (2009)
21. Hu, Y.-C., Wang, H.J.: A framework for location privacy in wireless networks. In: ACM SIGCOMM Asia Workshop (2005)
22. Chan, H., Perrig, A.: Security in Networks. IEEE Computer 36(10), 103–105 (2003)