A probability based hybrid energy-efficient privacy preserving scheme to encounter with wireless traffic snooping in smart home

Mohammad Ali Nassiri Abrishamchi, Abdul Hanan Abdullah,
Adrian David Cheok and Predrag K. Nikolic

Faculty of Computing, Universiti Teknologi Malaysia,
81310 Skudai, Malaysia
Imagineering Institute, Iskandar, Malaysia
City, University of London, London, UK

ali@imagineeringinstitue.com
Hanan@utm.com
adrian@imagineeringinstitue.com
predrag@imagineeringinstitue.com

Abstract. Application of pervasive computing devices in smart homes are rising sharply and due to this matter, demands for efficient privacy protection are increasing urgently. Possibility of interference in wireless networks is proved by previous work. Adversaries can discover contextual information because of traffic monitoring and classifying transmitters based on their radio fingerprints while data packets are encrypted or content is not important for attackers. To conceal communication patterns various approaches have been investigated. They are mainly based on injection of dummy packets into the network traffic and adding delay to transmission time. In this paper, we introduce a hybrid energy-efficient privacy preserving scheme for generating and sending dummy packets through a decision-making algorithm which works based on probability to maximize confusion of attacker in clarifying the real pattern of network traffic.

Keywords: internet of things, smart home, pervasive computing, privacy attack, daily living activities

1 Introduction

Smart home is one of the main applications of the internet of things. Low cost, sensory devices which can communicate wirelessly along with powerful capability of data processing are the key elements of this technology. However, these smart devices, in

some cases can work stand alone, but their true strength is in their collaboration with each other to form a network. In an ultimate smart home as a concept, every aspects of our life can be under observation of these smart devices, from our healthcare matters to details of our life style [1]. Gathering these sorts of data intends to be used for purposes of increasing the life quality. Having access to this kind of databases for authorized people can be helpful to have more control and make them capable of better management on their personal life. However, gaining access to these information is an interesting target for some unauthorized parties and it raises concern about privacy issue [2].

Like any other pervasive computing systems, in IoT, security and privacy considerations must come on the top of the requirements list, without paying attention to security matters, these system can be an interesting target for hostile parties, who are interested to steal data or interrupt services, for instance, hackers managed to took advantage of IoT devices to execute a Distributed Denial of Service (DDoS) attack in US by aim of interfering in US government online voting system for presidential election, IoT devices helped them to attack heavier and make the attack more difficult to stop [3]. This example shows why resolving security concerns has great impact in acceptance of smart home by users as a trusted system. Thus, confidentiality of personal data is highly demanded. While encryption techniques can provide a certain level of confidentiality for content of communications, they are not able to protect all aspects of privacy requirements. Context data is the uncovered section of privacy considerations in case of encrypted data. Context oriented privacy concerns about identity of communicators, their locations and their temporal information rather than the content of the messages they exchange [4].

Ad-hoc networks, 3G access network and WiFi networks are frequently used in smart home application and their nature of being infrastructure less and their vulnerability in providing context oriented privacy, makes them a suitable target for Side Channel Attacks [5]. A Side Channel Attack normally uses indirect ways by analytic/statistical approaches to delve in the captured wireless signals and discover meaningful sensible information, such as political opinions, lifestyle, medical records or financial details which can be transferred to a second party without the consent of individuals, leading to spam and other problems. This type of attacks are applicable for Activities of Daily Living (ADL) detection attack within a smart home [6].

An adversary tries to capture transmitted wireless signals by placing one or more signal sniffers about the smart home. Consequently whenever smart devices send a message to their destinations, an attacker can have a copy of those signals. Even if the content of messages be well protected by appropriate encryption algorithm, still there are possibilities for the attacker to analysis contextual data to identify the smart devices, and ultimately form a comprehensive map of the smart home network. In the next stage, every

activity inside the home can be detectable by the attacker and lead to privacy violations [7].

Studying existing solutions in similar domains such as wireless sensor networks and MANET shows those approaches cannot be applied directly into the domain of smart home due to producing undesirable extra delay or increasing the energy consumption [8], [9]. Thus, in this paper, we propose a Hybrid Energy-Efficient Privacy Preserving Scheme which is improved version of dummy packet injection approach [10], [11] and a random timing interval generator for determining the transmitting slot. Suggested solution is a decision-making algorithm based on probability theorem and it works by aim of maximizing the confusion level of the attack in its way to discover the correct pattern. These improvements are to avoid exorbitant energy consumption by continuous dummy packet generation, and prevent of undesirable delay for delay-sensitive devices. The proposed approach is basically a decision-making algorithm. Each smart device within the smart home should use this algorithm to decide about number of fake packets and time interval of transmitting them.

The rest of paper is organized as following: In section 2, process of fingerprinting and time snooping attack is reviewed. Section 3 illustrates the idea of the proposed technique. Section 4 presents a discussion of effectiveness of the proposed approach with summarized related work, and in Section 5, the conclusion is discussed along with potential future works.

2 Background

A side channel invasion is a Wireless Snooping Attack that tries to exploit contextual data of a network traffic instead of being concern about content of messages [12]. This sort of passive attacks is not detectable by any detection system, and attacker performs as a hidden silent observer to collect needed data. Disastrous results of this type of attacks, such as transferring the data to other parties from criminal organizations to insurance companies or spammers without permission and consent, cannot be avoided because the victim does not know when the attack is happening [13]. Fingerprint and Timing-based Snooping (FATS) is a robust attack to make adversaries able to capture wireless signals emitted from a smart home from somewhere outside of the home and stay undetectable as a nature of any kind of passive attacks [10]. Attackers interfere signals for a while and once the algorithm is trained enough, identities of smart devices and their locations will be clear, afterward, daily activities of residents of the home will be observable for attackers. FATS attack is based on wireless fingerprints and time monitoring of communications within the smart home [12], [14].

Wireless fingerprint is a physical characteristic of radio frequency-based communications which can be used to differentiate between different radios. And it is possible if even those devices being made in similar model and same manufacturer [12]. In addition, attack algorithm uses timestamps on each captured signal to be able to discover correlation between them. Moreover, time intervals will be used to measure distance of each smart device to the attacker's RF signal sniffer. FATS Algorithm has four stages which are explained as follow:

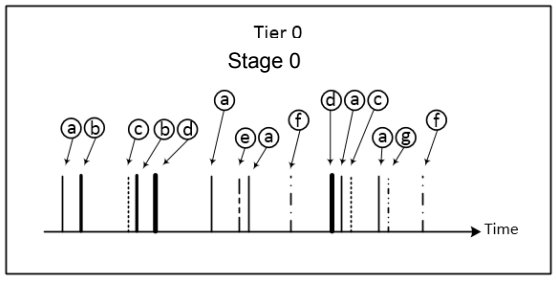
Stage 0 – Device detection*:* At the beginning, adversary can use radio activities, needless of fingerprints. Consequently, some basic activities are detectable, such as presence of residents which is referred by home events, sleep events or away events when home is not occupied. This stage is applicable on many homes which are using some basic wireless devices nowadays, despite they are not considered as smart homes. Later captured signals which are representing activities will be labeled to identify different transmitters. This stage is illustrated in Fig. 1. Stage 0.

Stage 1 – Device grouping: Attacker performs this stage by aim of discovering coexistence of devices in same room. For this purpose, calculation of temporal distance for each transmitter and if close devices in same room work by relatively short time difference makes them able to form clusters of devices. Fig. 1. Stage 1.

Stage 2 – Room function detection: Feature analysis is the key part of this stage, a bi-partite matching classifier labels each group of sensors according to their identified function, such as bathroom, kitchen, living room and etc. Fig. 1. Stage 2.

Stage 3 – Device Identification: A two-step classifying process is needed in this stage to clarify the identity of each device to label them as a stove, coffee maker, lighting system or refrigerator. Fig. 1. Stage 3.

Once the labeling is completed successfully, almost every activity in the target home is detectable in real-time [8], [14],[15]. Fig. 1, illustrates the flow of the FATS attack.



Stage 1

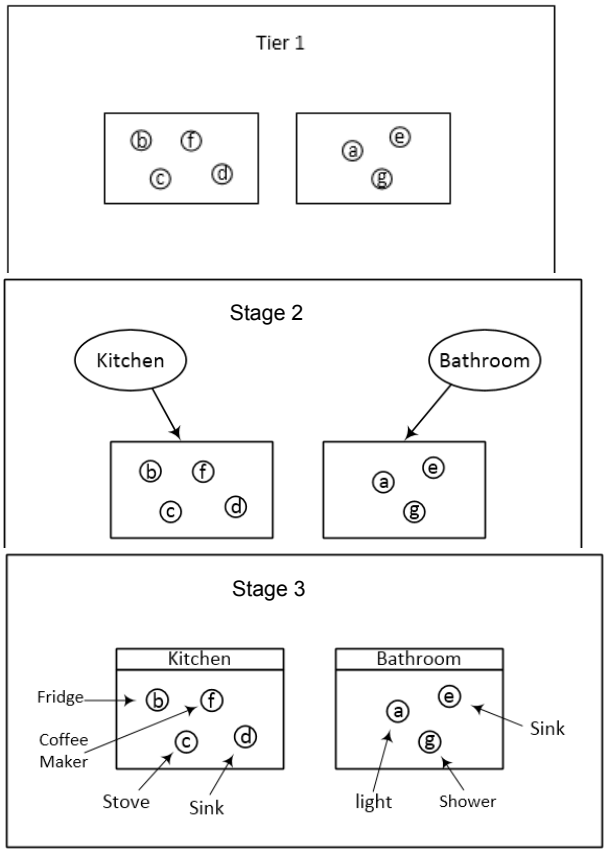


Fig. 1. Four stages of fingerprint and time snooping attack.
(a, b, c and etc. define unique wireless fingerprints)

3 Hybrid Energy-Efficient Privacy Preserving Scheme

FATS attack falls into category of global eavesdroppers, in this group of attacks, adversary can monitor the whole network activities and extract some critical secure information by applying pattern recognition techniques and traffic analysis. These attacks do not have any signs in the time of perform. Thus, victim has no chance to react in the same time [9]. To react to this vulnerability, a smart home can be ready all the time to encounter with the passive attacks to be able to preserve the privacy, just in case of incident. However, the attacker can monitor network activities but extracting meaningful information will be more challenging for them due to the permanent protection shield

which produce high level of randomness. To cope up with this problem, two major approaches are dummy packet injection and extra delay for transmitting the real data.

In dummy packet injection approach, sensor nodes are generating number of fake massages, exactly like real packets. Because the adversaries are not able to be informed of the content of packets, which are encrypted, they would not be able to differentiate between received packets. In the other hand, sink nodes of the network can detect and discard fake packets. It seems maximizing the number of dummy packet is an effective solution [11], [16]. But exceeding energy consumption is a serious barrier to let this method become a practical solution. There should be an optimal tradeoff between privacy level and energy consumption.

In the extra delay based approach, sensors avoid of transmitting the packets in their real-time. Adding delay can cause difficulties of in attacker's temporal analysis [15], [16]. However, if sensors try to use similar pattern of adding delay or considering a fixed time slot to send packets, there is possibility for adversary to cope with this solution. Moreover, in case of smart home, minimizing of delay due to existence of some healthcare monitoring system and emergency detection systems is not preferable. Fig. 2 shows how a real packet should wait for next time slot which can generate significant delay in total.

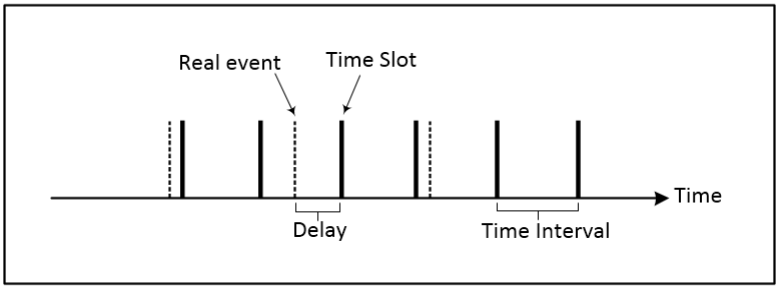


Fig. 2. Delay based solutions for encounter with global eavesdroppers.

However, even each of mentioned approaches are proposed for wireless sensor networks application they cannot be applied on smart home directly due to producing daily and extra energy consumption. In this paper, we are proposing a solution which is based on a combination of fake packets injection method and a variant time interval generator that the scheme decides about time slots for transmitting fake packets. Hybrid Energy-Efficient Privacy Preserving Scheme works based on the following principles:

- All real packets will be transmitted immediately to avoid any delay in sensitive cases.
- After every transmission, a random interval time will be generated to send a fake packet. In this way, system tries to avoid any certain patterns in sending the packets.

Maximum of time range (***t***) can be decided by system designer based on application and preference in terms of tradeoff between privacy level and energy consumption.

- When the waiting time for time slot is passed, a probability based decision making eavesdroppers algorithm, determines if the fake packet should be transmitted or it has to wait for next slot. In this step, a random number generator generates between zero and one, the generated number will be compared with the passing number (***p***) which is adjustable by system designer to control the rate of fake packets. For example, if the passing level is set on 0.5, each fake packet has 50% chance to be sent.

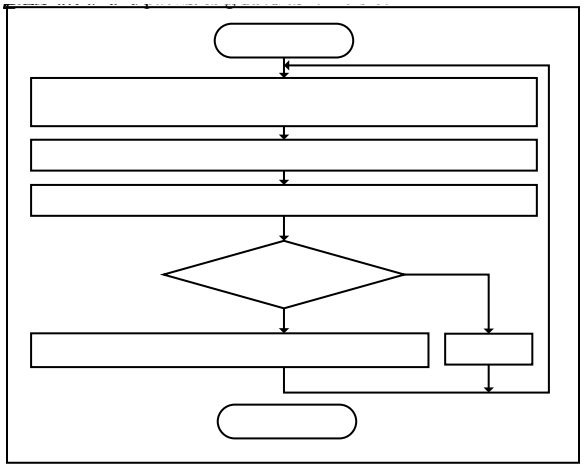


Fig. 3. Algorithm of Hybrid Energy-Efficient Privacy Preserving Scheme (***p*** is passing number and ***t*** is maximum of time range)

This solution allowing us to optimize the output in two stages in terms of number of fake packets and in regard with energy consumption. It suggests an adjustable tradeoff between privacy preservation level and energy consumption with zero additional delay for real packets.

In our solution, real packets have priority, but when there is no event to report, each device in smart home try to make some fake stream of data packets to provide higher level of privacy protection by decreasing the correctness rate of FATS attack's result for the adversary. As it mentioned earlier, the privilege of the proposed algorithm is in its flexibility and potential for optimization to find minimum needed dummy packets to provide a desired level of privacy preservation. Flowchart of this approach is shown in Fig. 3.

4 Research Approach

Our research approach for the solution evaluation consist of deploying a smart home as a testbed for our research. Numbers of smart devices will be installed in the home to report every event to the control center. Also, two wireless signal sniffers will be provided, one as an authorized sink node in smart home to log every reported event by sensor nodes and it performs the role of control center. And the other one represents the attacker's tool to intercept signals without any awareness about the list of existing devices. Because the first signal sniffer has an accurate lookup table to detect each transmitter precisely. Thus, after test, a log file with 100% accuracy will be available. In this round of test, smart home does not use any privacy protection method. At the same time, attacker executes the FATS attack from somewhere outside the home but in wireless signal coverage. Output will be a list of detected activity by attack algorithm. By comparing two files from both signal sniffer, we can determine the percentage of accuracy for FATS attack [14]. In the second round of the test, all sensor nodes are going to use Hybrid Energy-Efficient Privacy Preserving Scheme for each firing. Same as previous round, authorized signal sniffer and attacker's one will provide two lists after test. Comparison between these two lists shows the rate of correctness of FATS attack. At the end, the expected result is showing significant difference between two attack correctness rates, recorded from two execution rounds. Reduction in correctness rate, literally means higher privacy level for smart home. Fig. 4. Illustrated the evaluation concept.

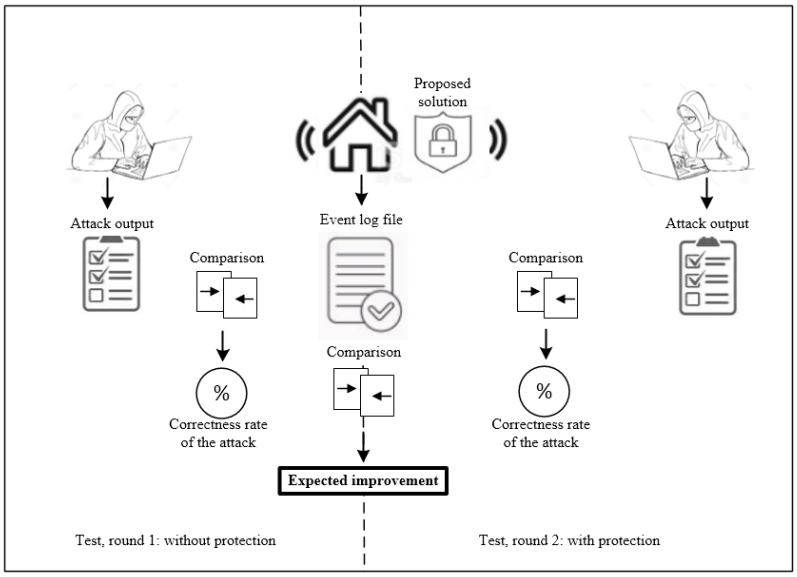


Fig. 4. Implementation and evolution approach

5 Conclusion

Living in smart environment will be almost unavoidable in future regarding to the current speed of IoT application growth. Providing reliable privacy level is one of the most important requirements. Privacy attacks such as FATS attack and similar attacks are serious threat for any type of smart environment from homes, offices to sensitive organization buildings or factories. This paper introduces a Hybrid Energy-Efficient Privacy Preserving Scheme as a defensive solution to encounter with FATS attack for smart home. In this work main objective of research approach is reducing the correctness rate of the attack algorithm which means increasing the privacy level, literally. We believe that proposed hybrid scheme, which combines fake data injection with random interval determination for time slots to transmit dummy packets, will reduce an adversary chances to discover the meaningful patterns for detecting in-home activities. What we also consider as an important issue is to provide a trade-off between privacy level and energy consumption rate via two adjustable system parameters which are t (random interval time for transmission slot) and p (probability based filter for fake packet injection). In the future, we are planning to extend our implementation of Hybrid Energy-Efficient Privacy Preserving Scheme to multiple types of smart home to collect data sets and evaluate efficiency of the method as well as optimizing our scheme for finding the best setting for the system parameters.

REFFERENCES

1. Stojkoska, B.L.R. and K.V. Trivodaliev, *A review of Internet of Things for smart home: Challenges and solutions.* Journal of Cleaner Production, 2016.
2. Choe, E.K., et al. *Living in a glass house: a survey of private moments in the home*. in *Proceedings of the 13th international conference on Ubiquitous computing*. 2011. ACM.
3. *Hackers Used New Weapons to Disrupt Major Websites Across U.S.* The New York Times, 2016.
4. Lin, H. and N.W. Bergmann, *IoT Privacy and Security Challenges for Smart Home Environments.* Information, 2016. **7**(3): p. 44.
5. Jing, Q., et al., *Security of the internet of things: Perspectives and challenges.* Wireless Networks, 2014. **20**(8): p. 2481-2501.
6. Zhao, K. and L. Ge. *A survey on the internet of things security*. in *Computational Intelligence and Security (CIS), 2013 9th International Conference on*. 2013. IEEE.

7. Lu, J., Y.T. Shams, and K. Whitehouse, *Smart Blueprints: How Simple Sensors Can Collaboratively Map Out Their Own Locations in the Home.* ACM Transactions on Sensor Networks (TOSN), 2014. **11**(1): p. 19.
8. Park, H., et al., *Energy-Efficient Privacy Protection for Smart Home Environments Using Behavioral Semantics*. Sensors, 2014. **14**(9): p. 16235-16257.
9. Nassiri Abrishamchi, M.A. and H. Chizari, *AN OVERVIEW OF SOURCE LOCATION PRIVACY IN WIRELESS SENSOR NETWORKS AGAINST GLOBAL ADVERSARY.* Asian Journal of Mathematics and Computer Research, 2016. **8**(3): p. 12.
10. Chow, C.-Y., W. Xu, and T. He, *Privacy Enhancing Technologies for Wireless Sensor Networks*, in *The Art of Wireless Sensor Networks*. 2014, Springer. p. 609-641.
11. Ngai, E.C.H., *On providing sink anonymity for wireless sensor networks.* Security and Communication Networks, 2016. **9**(2): p. 77-86.
12. Xu, Q., et al., *Device fingerprinting in wireless networks: challenges and opportunities.* IEEE Communications Surveys & Tutorials, 2016. **18**(1): p. 94-104.
13. Kapetanovic, D., G. Zheng, and F. Rusek, *Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks.* IEEE Communications Magazine, 2015. **53**(6): p. 21-27.
14. Srinivasan, V., J. Stankovic, and K. Whitehouse. *Protecting your daily in-home activity information from a wireless snooping attack*. in *Proceedings of the 10th international conference on Ubiquitous computing*. 2008. ACM.
15. Park, H., T. Park, and S.H. Son, *A Comparative Study of Privacy Protection Methods for Smart Home Environments.* Int. J. Smart Home, 2013. **7**: p. 85-94.
16. Conti, M., J. Willemsen, and B. Crispo, *Providing source location privacy in wireless sensor networks: a survey.* IEEE Communications Surveys & Tutorials, 2013. **15**(3): p. 1238-1280.