6-28-2016

Secure Communication Scheme in Smart Home Environment

Hari Krishna Jonnalagadda
University of South Florida, hari.jonnalagadda8@gmail.com

Secure Communication Scheme in Smart Home Environment

by

Hari Krishna Jonnalagadda

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Computer Science
Department of Computer Science and Engineering
College of Engineering
University of South Florida

Major Professor: Yao Liu, Ph.D.
Yicheng Tu, Ph.D.
Jay Ligatti, Ph.D.

Date of Approval:
May 26, 2016

Keywords: Security, Accelerometer, Gravity, Authentication, Automation

DEDICATION

I would like to dedicate this thesis to my family, who stood by my side in all my endeavors. I would like to dedicate a part of this thesis to Dr. Srikanth Jatla, Director, Aurora Technological and Research Institute, who inspired me for life time with his teachings.

ACKNOWLEDGMENTS

I acknowledge Dr. Srinivas Katkoori, Graduate Program Director (Fall 2015, Spring 2016), Department of Computer Science, for his extensive motivation and support, which provoke me to initiate my thesis.

I acknowledge Dr. Yao Liu, major professor, for directing the research behind this thesis. It's been a great pleasure to work with a professor, like Dr. Liu, who continuously keeps me motivated and provided enough space to explore new ideas.

I acknowledge Nagalaxmi Yenuganti, my co-student, who contributed by providing her views all through my research. I acknowledge her work in designing an Android Application, which we used to perform experiments.

I acknowledge complete research team directed by Dr. Yao Liu; Ian Markwood, Song Fang, Tao Wang, Dakun Shen, Zi Li and Ahamad Alagil for providing feedback on my research, which really helps to enhance my research.

I acknowledge Dr. Jay Ligatti and Dr. Yicheng Tu for serving as committee for my Master Thesis.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Internet of Things, has started to mark its existence from past few years. Right from its inception with a coke machine at Carnegie Mellon University, it has come a long way, connecting billions of devices to internet. This journey is well supported by the advancements in networking, hardware miniaturization and sensing capabilities.

Diverse nature of applications of Internet of Things, has cut the communication barriers between the varieties of fields ranging from manufacturing industry to health-care industry. Smart Home is one such application of Internet of Things. Connectivity of home appliances, to achieve automation in living, defines Smart Home. Out of welter of applications that are derived from Internet of Things, this thesis concentrates on Smart Home. Smart Home, in practical is expected to conserve lot of energy, by achieving automation of home appliances, on par with best living experience.

Existing technologies such as Z-wave, One-Net, ZigBee, Insteon, had already occupied the Smart Home communication. However, these technologies face the problem of identifying the smart devices uniquely and also exhibit security vulnerabilities. Proposed scheme exploits accelerometer fingerprinting to identify the smart devices uniquely. Security vulnerabilities of existing protocols are addressed by encrypting the data on move with CCM mode of AES encryption.

CHAPTER 1:

INTRODUCTION

Internet of Things [1] has started to mark its existence since few years. Today, high network bandwidth, cheaper and high sensing capabilities, miniaturization of hardware, made Internet of Things visible. Communicating with non-living things had become reality. It is observed by cisco systems that, in 2008, the number of devices that are connected through internet had exceeded the number of people living on the earth [2]. By 2012, the count reached 1.5 times the number of people [2]. This trend is expected to grow exponentially and by 2020, the count of the devices that are connected, reach 50 billion, make the ratio of people to connected devices as 1:8 [2]. It is also estimated that by 2020, every person in the world, will communicate with average of 3000-5000 devices around him [3]. Under the cover of Internet of things, when all the things are virtually connected to each other, and are able to communicate with each other, then automation is very much possible. Someone, need not think of refueling car, washing clothes, driving a car, taking pet for walk, making coffee, adjust room temperature, switch off lights and call for emergency and what not? Despite advancements in Internet of Things, the problems of security and privacy are always present. In fact, the major problem that slows down the penetration of IoT in to current world is security.

Security is always an enemy, for any technological advancement in the industry, but is of great concern. Suspension of production of Google glass [4], could be a good example. As there is increase in the number of devices that communicate, it is expected that the data that is transmitted over network increases enormously. As of 2012, Google search is capable of searching the data

which is approximately equal to 4000 Exa-bytes (stack of books from earth to Pluto eighty times) [3]. Facts leaves a big challenge of secure data on move.

Addressing any of the issues, will root back to one major problem of identification of devices uniquely. We could see many techniques, to identify the devices uniquely, such as UDID [5], Mac address [6], Serial number [7], Device ID [8]. These techniques are either used for identifying proprietary devices or can be easily spoofed. We provide concrete evidences of how existing techniques fail to identify devices categorically. Accelerometer fingerprinting [9] had provided, a different and concrete way of identifying devices uniquely. We exploit this technique to provide a secure communication in smart home environment.

Smart home [10] is one of the applications of Internet of Things. Smart Home is a technology, where all the devices in home, communicate to each other so as to achieve automation. It seems orthodox, that when we wake up, the room temperature is adjusted automatically, bed coffee is ready for us in the coffee machine, water will be warm/cool based on the room temperature, your phone prepares schedule for day, switches off the electric fan and light the moment you left a room and what not? Smart Home thus, provides user friendly environment.

This thesis focusses on generating unique cryptographic keys for smart devices, which can also be used to identify the devices uniquely. This thesis also focusses on providing secure communication in smart home environment. The organization of the document is as follows. Chapter two will provide architecture of smart home environment. This chapter also provide security schemes that are feasible in smart home environment. Chapter three will provide new way of generating True Random Numbers called Accelerometer Fingerprinting. This technique is used to identify smart devices uniquely, in proposed method. Chapter four will provide information about the existing security protocols that are employed in smart home. This section also provide

certain short comes of existing protocol, which are addressed by proposed method. Chapter five will provide proposed security system for smart home environment. Chapter six will provide strong defense for proposed scheme, by providing attack-defense models. Chapter seven will provide comparative analysis of proposed scheme and existing schemes in smart home. Chapter eight concludes the thesis by providing summary. Chapter nine provides some intuitions of future work to make smart home secure.

CHAPTER 2:

SMART HOME COMMUNICATION AND SECURE SCHEMES

2.1 Smart Home Environment

Smart Home Environment is defined as home like environment that possess ambient intelligence and automatic control and capable of reacting to the behavior of residents and to offer various accommodations and is further divided in to healthcare based, multimedia based, security based, and energy efficient based [10]. Smart Home interconnection specifications and communication technologies are very new and relies more on local networks [10]. Health care based Smart Home, adapts Body Area Network (BAN) so as to monitor the health condition of people living inside the home [10]. Security based and Energy efficient based Smart Home, adapts Wireless Sensor Networks (WSN) to achieve automation, and provide better living experience for users [10]. Multimedia based Smart Home adapts Personal Area Network (PAN) to give user the best experience of electronic devices [10]. These diverse networks constitute to a concrete Home Area Network (HAN). Gateways based on Machine to Machine infrastructure, interacts with surrounding environment [10].

Due to diverse technologies that are adapted by Smart Home to achieve automation, we need controllers to negotiate the protocols that are adapted by these technologies. Typically, this controllers receives the data from all the devices, analyze them, and then take the necessary reactive measures to achieve automation.

Smart Home environment in not only restricted to achieve the automation based on the sensing data, but also expands towards the behavioral analysis of persons living in Smart Home

[10]. This behavioral analysis is done in the cloud, which receives the data from the sensing devices, through gateways provided by Machine to Machine infrastructure in Smart Home and analyze the natural habitat of people living in Smart Home [10]. Based on this analysis, cloud will provide the certain recommendations for the user for better living experience.

This thesis primarily concentrates on secure communication between the sensors in smart home and controller that analyze the data so as to provide energy efficient and secure smart home, with automation. As explained earlier these technologies use Wireless Sensor Network (WSN). This thesis is intended to provide a secure scheme to provide integrity and confidentiality of sensor data.

Figure 1 would depict the smart home architecture. This figure shows different networks in smart home and their communication interfaces. Health care of user is monitored through Body Area Network (BAN). Surveillance, security and energy management are controlled by Wireless Sensor Networks (WSN). User personal entertainment can be monitored and controlled through Personal Area Network (PAN). All these networks are integrated by wired or wireless interfaces to provide automation. Figure 1 also provide some of the existing protocols that provide automation. M2M infrastructure in smart home acts as gateway to outside environment. Cloud which receives the data from all the surrounding networks would provide early recommendations to the user, to provide smart life.

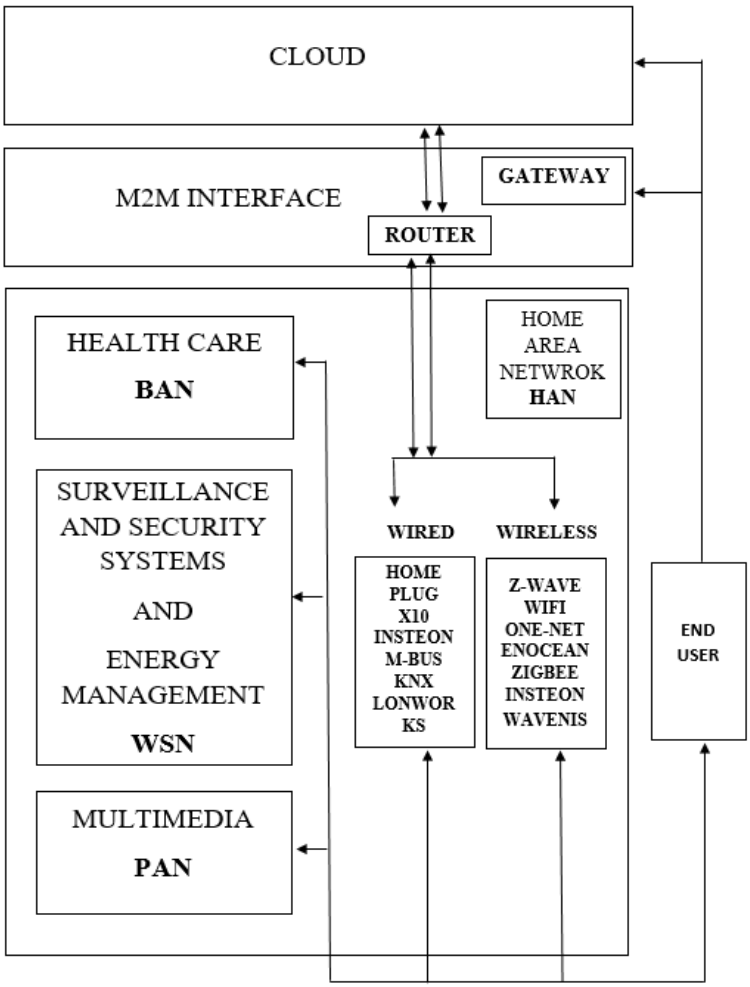

Figure 1: Smart Home Architecture

Devices in smart home environment are constrained in memory and computational capacity. Smart home can adapt only light weight schemes, as devices are constrained. Section 2.2 provides secure communication schemes and their feasibility in smart home environment.

2.2 Secure Communication Schemes

This section aims to provide basic security schemes that are widely used in network of nodes. This section also provides the information about what scheme could be best suitable for Smart Home environment.

2.2.1 Symmetric Cryptography v/s Asymmetric Cryptography

In the world of cryptography, we had two major schemes that ensures the confidentiality of data on move, namely symmetric cryptography [11] and asymmetric cryptography [11].

Symmetric cryptography is scheme, where same key is used to encrypt and decrypt the data. Symmetric encryption is light weight encryption scheme. Security of symmetric cryptography lies in the shared secret key. Advanced Encryption Standard (AES) is most secure symmetric encryption standard till date [12].

Asymmetric cryptography is scheme, where each communicating peers will have a public and private key pairs. Public keys are used to encrypt the data and private keys to decrypt data. For example, if node 'A' wishes to communicate to node B, A will encrypt the data with the public key of node B and can send cipher-text over insecure channel to node B. On the other end, node B decrypts the received cipher-text with its own private key. Public keys of all the nodes are known to every other node, whereas private keys are completely private to the nodes. It is claimed to impossible to decrypt the cipher-text, which is encrypted with public key, without private key.

Smart devices or sensors in smart home can adapt only to symmetric encryption, due to their low computational capacity. One problem that still haunts is sharing a secret key between the communication peers. Nevertheless, symmetric encryption is light weight solution, and is feasible for providing confidentiality in smart home network.

2.2.2 Authentication of Sensors in Smart Home

Secure communication in Smart Home includes identifying the legitimate sensors in home environment. An anonymous sensor node can impersonate the communication in home environment and can get access to private data. Secure schemes has to identify such anonymous nodes, to ensure secure communication. Techniques like linking control, can restrict the

communication to legitimate nodes, by identifying them with unique identifiers. There are many existing techniques to identify a device uniquely, such as, Device ID [8], MAC address [6], Serial Number [7], UDID [5]. Despite many techniques to identify a device uniquely, every technique has limitations. For instance, Device ID is the identity used for the devices with telephony capabilities [8]. We cannot expect to have the telephony capabilities for all the devices in Smart Home environment. MAC address is the physical address of a device, this address can be changed by the owner of device [6]. Unique identifier is expected to be same throughout the life cycle of device and hence MAC address could not be used as unique identifier. Serial Number can be used as unique identifier, but it is available only in the later versions of smart devices [7]. UDID is the unique identifier for devices from Apple Inc, but this UDID is deprecated in later versions of Apple software [5]. All the above mentioned schemes are machine generated and are Pseudo Random Number Generators (PRNG's). In this thesis, we provide a different scheme to identify the devices uniquely, by exploiting the manufacturing errors. Manufacturing errors are not only more random, but also provide high uniqueness compared to PRNG's. Analysis of Pseudo Random Number Generators (PRNG) v/s True Random Number Generators (TRNG) are described in following section.

2.2.3 Pseudo Random Number v/s True Random Number

Pseudo Random Number Generator (PRNG's) v/s True Random Number Generator (TRNG) is an interesting debate in cryptography. Quite often than not, it is the tradeoff between the randomness and cost of generating. PRNG's are easier to generate, but fails to provide complete randomness [13]. On the other hand TRNG's are difficult to generate, but could provide complete randomness.

Pseudo Random Numbers are the numbers that are generated by an algorithm, which makes them deterministic. This enforces security algorithms to use large key bit sequences, so as to increase sample space of possible keys. Pseudo Random Numbers can easily be substituted with True Random Numbers, if TRNG's are made cost effective and resilient to side-channel attacks.

True Random Numbers on the other hand are highly random and are non-deterministic. The randomness and non-deterministic nature of True Random Numbers motivates to substitute Pseudo Random Numbers. We provide light weight solution to generate True Random Numbers by exploiting manufacturing errors.

Smart home environment in addition to automation, interfaces with outside environment. Based on increasing trend of acceptance of smart home technology, smart devices are expected to communicate with large number of devices in and around home environment. This fact motivates to identify the devices with True Random Numbers, which promises high uniqueness and randomness.

CHAPTER 3:

ACCELEROMETER FINGERPRINTING

As discussed in section 2.2.3: it is True Random Numbers that fits in the context of Smart Home. In this section we propose a unique way to derive True Random Number. True Random Number is defined by the probability of recurrence of bit sequence in a sample space is nearly equal to 0. Pseudo Random Number, being generated by deterministic algorithms, which follows a specific pattern, fails to provide complete randomness.

Unlike, existing schemes, proposed scheme generate keys through True Random Number Generators. Every device in smart home environment is expected to be identified uniquely by the controller node or by the cloud. With increasing number of devices that are connecting to Internet where randomness in keys is on demand, existing key generation techniques which rely on PRNG's might lose their integrity.

3.1 Different Ways of Generating TRNG's

True Random Numbers can be derived through various ways. One of the easiest way is to maintain a counter, where in each time you increment the counter to derive the new number, different from previously derived random numbers. This scheme would provide complete uniqueness by fails to provide randomness. In context of cryptography this provides very minimal security. Intruder can easily guess the next key bit sequence, as it is one more than previous key bit sequence.

The most significant way to create a True Random Number is through the manufacturing errors of a device. To fit the context, we could consider the manufacturing errors of the sensors. It

is a well-known fact that, any device is prone to manufacturing errors and these errors are completely random, assuming the proper functionality of manufacturing machinery. As these errors are completely random and are non-deterministic, they can generate True Random Numbers.

3.2 Dependency Problem

Unique identifiers should be easy to generate and consistent throughout the lifetime of device. We need a location specific constant entity, against which we can calibrate the device to derive manufacturing errors. For instance, it is difficult to calibrate the manufacturing errors of temperature sensor, as the temperature at a specified location is not constant. One entity, which is constant at specific location is acceleration due to gravity 'g'. Acceleration due to gravity on a device can be measured with accelerometer. Manufacturing error of accelerometer can be used to generate True Random Numbers.

3.3 Accelerometer Fingerprinting

Accelerometer fingerprinting [9] is a technique of identifying the devices uniquely, based on the manufacturing errors of the sensor called accelerometer. Accelerometer is a sensor which measures the acceleration due to gravity [14], which is constant at specified location. Most of the electronic devices, today are equipped with the accelerometer circuitry, and is exploited in various ways. There might be few devices which might not be equipped with accelerometer circuitry, this problem can be solved by installing an Arduino, which can act as accelerometer. With rapid change in Internet of Things, we can expect minimal die area of Arduino, which provide the functionality of accelerometer. It will be even more efficient, if manufacturers, could go a step ahead, and provide the accelerometer functionality in the chip of device, as the die area of accelerometer would be few millimeters [15]. Every device is equipped with accelerometer, could be a strong

assumption, but minimal die area and promising fingerprinting through manufacturing errors of accelerometer, support accelerometer fingerprinting to generate TRNG's.

3.4 Experiment Conducted to Provide Correctness Proof of Accelerometer Fingerprinting

Calculating accelerometer errors in smart home devices would be extremely time taking. We chose smart phones to demonstrate accelerometer fingerprinting, because accelerometers would show manufacturing errors in any of the smart devices they are installed on. Smart phones are equipped with accelerometer circuitry. Despite the fact that this experiments are performed by [9], we choose to perform them again to measure the accuracy of the results. We developed an android app, which acts as an interface with the accelerometer circuitry. We took the advantage of the interface called SensorManager in Android, which provides the data of all the sensors that are in smart phone. With the help of this app, we are able to store the values of acceleration of smart phone in all the three coordinate axes (X, Y, and Z).

3.4.1 Experimental Setup

Experimental setup for the correctness proof of accelerometer fingerprinting very simple. All we need to have is a plane stable surface and smart phone with accelerometer app installed on it. Smart phone, when placed on plane surface without any physical movement, would result in the acceleration only in perpendicular direction to surface of contact. This acceleration is typically equal to the magnitude of acceleration due to gravity at the location of experiment. We can monitor the acceleration of smart phone in all three directions with the help of app. Data record from the data set of accelerometer readings should ideally show (0, 0, value of g) corresponding to (X, Y, Z) axes. Due to inherent manufacturing errors in devices, they show variation in the readings. We perform similar experiment with various smart phones to provide strong evidence that manufacturing errors would produce True Random Numbers.

Figure 2 shows the experimental setup. A smart phone is placed on plane surface, without any physical motion. Figure also shows accelerometer app installed in smart phone. This experimental setup is to demonstrate accelerometer fingerprinting. We chose to use smart phone, as it is easy to interface underlying sensors in smart phone. Accelerometers in any of smart devices would exhibit similar fingerprinting, as they exhibit in smart phones. Hence, keys derived from accelerometer fingerprinting are expected to be completely random. Figure 3 which shows the results of fingerprinting, which certify the fact that keys derived from manufacturing errors are completely random.

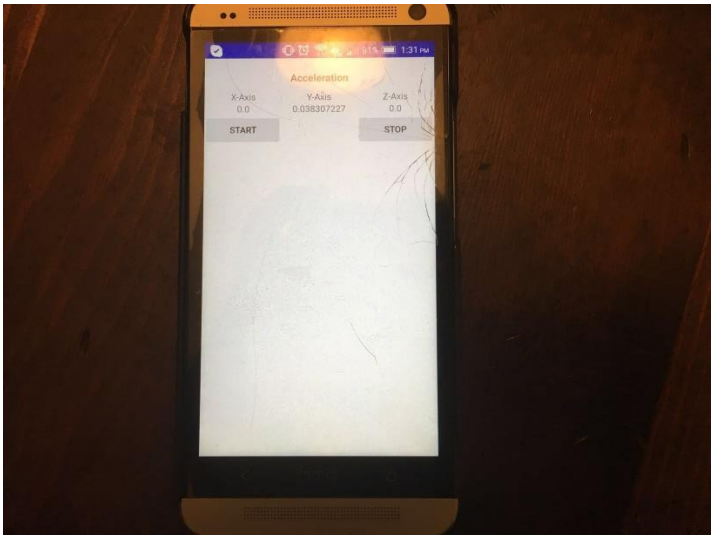

Figure 2: Experimental Setup

3.4.2 Location Specific 'g' Value

Acceleration due to gravity changes from location to location [14]. In fact the acceleration due to gravity is the resultant acceleration of all the force of attractions that acts up on body. Standard gravity of earth measured at sea level is 9.8 m/s^2. The value of 'g' can vary with elevation of location above sea level, tidal impact, local gravity variation and latitudinal position [14]. Out

of these the most significant change can be visible only when there is change in latitude. All the other factors might constitute to ± 0.0006 m/s^2 [14]. As this value is very minimal, we ignore this change and calculate the manufacturing errors based on latitudinal changes. All the experiments of this thesis are conducted in Tampa, Florida, USA. As per the approximation provided by [14], the acceleration due to gravity at Tampa is measured as 9.79169 m/s^2.

3.4.3 Quantization of Accelerometer Error

Quantization of accelerometer error is done similar to proposed method in [14]. To calculate the error of accelerometer, we need to calculate the offset of device. We calculate offset using following formula.

$$Z_m : O_Z = Z_m - (g * S_z)\ [14] \qquad \text{---------- (1)}$$

O_z, represents the offset of error, calculated from accelerometer in Z-direction [14]. Z_m represent the measured 'g' value from accelerometer. 'g' represents acceleration due to gravity corresponding to the location of experiment. S_z represents the sensitivity of accelerometer error.

Offset of an error corresponding to any axis requires sensitivity of accelerometer. Sensitivity of accelerometer can be calculated by taking the values of the accelerometer while the smart phone is both directions i.e facing upwards (Z_{m+}) and facing downwards (Z_{m-}) [14]. Sensitivity of accelerometer is provided by following formula

$$S_z = (Z_{m+} - Z_{m-})/2g[14] \qquad \text{---------- (2)}$$

From eq 1 and 2 we get $O_z = (Z_{m+} + Z_{m-})/2$ [14]

We calculated the offset values of 7 different android smart phones, the results turn out to be promising for accelerometer fingerprinting. We plot these values so as to provide the confidence on accelerometer fingerprinting, which in turn results in generating True Random Numbers. Figure 1 would depict the accelerometer fingerprinting very precisely.

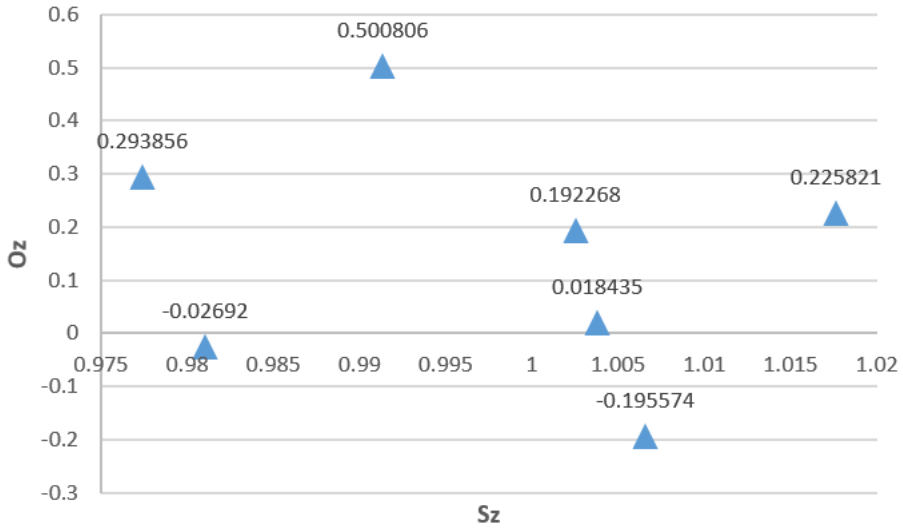

Figure 3: Accelerometer Fingerprinting

The above figure would demonstrate the accelerometer fingerprinting [9]. This graph is plotted between the sensitivity of the accelerometer sensor and corresponding offset in Z-direction. As we could see that no two accelerometers would result in same offset value, we claim that no two accelerometers can have same manufacturing errors. Similar experiments can be conducted along other coordinate axes. Similar experiment is conducted on 16000 smart phones by [9]. Results of this experiment clear provides randomness of manufacturing errors, and thus support accelerometer fingerprinting.

A key bit sequence can be generated from accelerometer fingerprinting by various key generation schemes such as quantization techniques. As these key bit sequences are generated from the manufacturing errors of accelerometer, they are True Random Numbers.

CHAPTER 4:

EXISTING PROTOCOLS AND THEIR SHORT-COMES

Smart home automation completely relies on the secure communication between the devices and smart home controller. Smart home controller provide communication interface between varieties of devices in smart home. Some of the existing protocols in smart home environment that provide communication interface to achieve automation are Z-wave [16], ONE-NET [17], ZigBee [18],[22], Insteon [19],[20] etc. We provide details of existing protocols, before proposing our scheme.

4.1 Existing Protocols

4.1.1 Z-Wave

Z-wave is proprietary Smart Home automation technology, developed by Zen-sys, later acquired by Sigma Designs. Z-wave's primary concerns was about control lighting, HVAC and security. Z-wave infrastructure includes a controller to control the communication of devices in the Smart Home. Each device is configured and assigned a Node ID [21]. A unique Network ID is assigned to controller of every Smart Home [21]. The Z-wave network can be uniquely identified by the Network ID, which is derived from hardware based PRNG [21]. The security between the devices and controller is promised by AES encryption [21]. This security is questioned against using the temporary hardcoded key to encrypt and decrypt key exchange packets, which leaves a vulnerability to the attacker [23]. Attack can be made even easier as this protocol do not provide the state validation during the key exchange [23].Due to its proprietary nature, this network cannot

be extended to the devices from other manufacturer. We propose a similar architecture in our secure smart home scheme, but proposed scheme can be extensible to devices from different manufacturers.

4.1.2 ONE-NET

ONE-NET [17] is an open source standard for wireless networking. This wireless standard, implements Tiny Encryption Algorithm to encrypt the messages between the communication nodes. 128-bit block cipher experienced duplicate keys and compromised security to an effective key length of 126-bit [24],[25],[26]. Even though, they find a fix for this vulnerability with the advanced version of XTEA [27], root cause behind the vulnerability is certainly usage of PRNG's as keys. Our approach will assure, complete randomness of key bit sequence, by exploiting accelerometer fingerprinting, a TRNG.

4.1.3 ZigBee

ZigBee [18],[22] is IEEE 802.15.4 specification suite for high level communication protocol. To ensure secure communication, ZigBee uses CCM mode of encryption [22]. CCM mode is combination of CBC-MAC mode and Counter Mode. Devices encrypt the sensor data with 128- bit block encryption technique, Advanced Encryption Standard (AES). Message is signed by generating Message Authentication Code (MAC) with Cipher Block Chaining (CBC) mode of AES [22]. Message and MAC are encrypted using stream cipher in Counter (CTR) mode of AES [22]. ZigBee uses three different type of keys to ensure integrity and confidentiality of messages namely, Master Key [22], Link Key [22] and Network Key [22]. Master Keys are installed in the devices, to provide protection for link keys. Link keys are used to encrypt the data between the nodes. Network key [22] is a unique key assigned to every node in the network, to recognize that all the nodes in network. As the number of nodes in the network increases, the

memory required to store the Master Keys, Link Keys and Network Keys increases. Our proposed method, will mitigate this effect to centralized node inside home environment, which is expected to have high configuration compared to the sensor devices. This approach also provides very low resilience.

4.1.4 Insteon

Insteon [19],[20],[21] is a home automation technology, where devices communicate synchronously over a dual mesh network that combines the RF wireless network and the electrical wiring. The dual band communication is to provide the integrity of communication between the devices. Security to bind the sensors to communicate among the sensors, inside the home is controlled by linking control [20]. Insteon technology can also adapt to centralize monitoring, with the help of central controllers. Each and every device is identified by unique identifier similar to MAC address [20]. Firmware would recognize the legitimate sensors based on the unique identifiers assigned to the sensors [20]. Whenever a new device is added to the existing network, user has to perform operations in the devices so as to configure it with the network. This approach demands user intervention to configure the device to network. This approach is not compatible with the devices, which do not provide user interface. Insteon [20] do not make any encryption, as the whole security is promised by the linking control provided by Firmware [20]. The security of Insteon is thus criticized by [28].

CHAPTER 5:

SECURE SMART HOME COMMUNICATION SCHEME

Existing secure smart home protocols had problems in either extending the compatibility to variety of devices or compromising the security, by week PRNG's. In addition to that using PRNG's to compute MAC of messages to provide the proof of message origin, is completely dependent on the randomness of PRNG's.

ONE-NET [17], which uses Tiny Encryption Standard, had faced problem of lack of randomness in the key, resulting in decrease of effective length of the key from 128-bits to 126-bits. The secure scheme we propose uses the TRNG by exploiting accelerometer fingerprinting.

Every device in the ZigBee [18], [22] protocol has the link keys of every link that device shares, gives no resilience on the attack. Compromised node in ZigBee would expose all the link keys to attacker.

Z-wave [16] protocol being a proprietary protocol, would serve only the devices that are from Sigma Designs. This approach would lead to partial automation of smart home, as only automation services by Sigma Devices are only achieved.

Insteon [19],[20],[21] protocol suffers the problem of human intervention while configuring a device to smart home network. Insteon in the name of linking control [20], do not use any encryption. This technique is criticized against security by [28].

Proposed scheme would solve the short comes of above protocols, based on strong assumption, that every smart device is equipped with accelerometer. We anticipate that minimal

die area of accelerometer sensor, should not be a barrier for penetration of proposed scheme in to the Internet of Things.

5.1 Topology

In proposed scheme, nodes communicate over mesh network. All the nodes in the home network will send their packets to centralized node called controller, through intermediate nodes. Centralized node which is capable of analyzing the data received, receives data from all the sensors in the home environment and take reactive steps to achieve automation. Intermediate nodes will only forward the packet, until packet reaches the centralized node. For instance, if node A wishes to communicate with the centralized node, it encrypts its packets with the secret key of centralized node and transmits packet through the intermediate nodes. Intermediate nodes, simple forward the packet, until packet reaches centralized node. Centralized node which is in possession of keys of all the nodes in the network can easily decrypt the message using the corresponding key of node. If centralized node wishes to send the packet to any of the nodes, it will encrypt the packet with key of corresponding node and forwards the packet to the node through intermediate nodes. Every node, will check if the packet sent by controller is intended to itself; if the packet is not intended to the node, it just forward the packet. If the packet is intended to itself, then packet is decrypted with its own key.

5.2 Secure Channel Establishment

To ensure confidentiality of data in move, we need to establish a secure channel between nodes and controller. As discussed earlier, public key cryptography is not feasible in smart home environment, we choose symmetric encryption. We use accelerometer fingerprinting to derive unique keys for nodes. Keys of all these nodes are to be shared with controller node. Secret key of controller has to be shared with every other node. Key exchange is extensively debated in the

symmetric cryptography, where no technique has ever promised the secure way of sharing secret key. Key exchange is a vital step in whole security system and has to be done in very secure way. We try to solve this problem by limiting the timing window for attacker to launch an attack. Every node should be configured to the network, to be identified as legitimate node. Key exchange happens during the configuration. It is most unlikely that attacker launches the attack during the limited time of configuration of device.

5.2.1 Key Generation

With the motivation of identifying all the nodes in the Smart Home uniquely and also to provide the high security, we opt for TRNG's to generate keys. Accelerometer Fingerprinting had provided, adequate randomness in keys and is also complex to re-generate same key. Each and every node in the Smart Home network is assumed to have accelerometer circuitry in their chip. With the help of diverse manufacturing errors that accelerometers would exhibit, we can easily identify the nodes uniquely. As the manufacturing errors are completely random, attacker cannot able to generate the same key bit sequence, in trail of mimicking the legitimate node. These manufacturing errors of accelerometers are hashed with an efficient hash functions to generate unique and secure bit sequences. Output of hash functions are used as keys for symmetric cryptography, to ensure confidentiality of communication.

5.2.2 Key Exchange

Nodes in the network generate the keys based on their accelerometer fingerprinting. To establish a secure channel between nodes and controller, keys has to be exchanged between all the nodes and controller. The key exchange has to be done through a secure channel. In proposed scheme, key exchange happens at the time of configuring a device to controller. Once the keys are exchanged, nodes in the network can communicate with the controller securely. As the

configuration of a node takes very minimal amount of time, we assume that attacker will have a very less timing window to launch an attack to retrieve keys. Controller also keeps track of node ID's and the keys of nodes. Hence, this also acts as an authentication for nodes in the network. This prevents unauthorized node communication in network.

5.3 Secure Communication

We had successfully established a secure channel between all the nodes and controller. All the communication between the nodes and controller happens through the established secure channel. Keys generated through accelerometer fingerprinting are used to encrypt the messages to provide confidentiality. Proposed method uses AES encryption to encrypt the data between nodes and controller. Nodes will encrypt the data with their own key and send to controller. Controller would decrypt the packet with the node keys, as key of every node is known to the controller. Similar to ZigBee [18],[22], we provide packet integrity by calculating MAC of packet using the Cipher Block Chaining technique. Message is now appended with the calculated MAC and encrypted with Counter mode of AES encryption. Cipher text thus generated is sent to controller through the intermediate nodes. Controller, which in possession of key of the node, will decrypt the packet. Controller will also calculate the MAC of the message and then compare the MAC it received, to ensure the integrity of message. Proposed method fairly mimics the ZigBee protocol, to provide integrity and confidentiality of data, but proposed method provides high resilience. We provide strong defense of proposed secure scheme.

5.4 Security of Proposed Scheme

Common traits in which security of system is questioned are against, confidentiality of the data in move, authentication of communication node, integrity of messages, availability. We defend our proposed scheme in following sections.

5.4.1 Confidentiality

Confidentiality of information plays a key role in Smart Home security. No user wishes to expose his way of living to the outside world. In the proposed scheme, communication between the nodes and the controller is encrypted using AES algorithm. For an attacker to crack the key used for AES encryption, he has to brute force AES algorithm by trying all 2^{128} possible ways of keys. Unlike Tiny Encryption Algorithm [24],[25],[26], the keys in proposed scheme are derived from manufacturing errors of accelerometers and hence provide complete randomness. Using TRNG's makes our approach robust, to create the random keys, unlike any other security schemes. Higher the randomness, more is time taken for attacker to crack the key. On top of it, we also use a very secure mode of encryption coupled with AES, AES-CBC-CTR. Using secure modes of operation provide high confidentiality of data.

5.4.2 Authentication

Authentication in smart home environment is identifying the legitimate nodes. In proposed scheme, every node in the network has to be configured with the controller. New nodes has to be configured at the time of installation. Controller will save the ID's and keys of all the nodes in the network during configuration. Attacker might introduce a malicious node to intercept the communication in the smart home, but this can be easily identified by the controller, as the key value of malicious node cannot be matched with the list of keys of legitimate nodes.

5.4.3 Integrity

Integrity plays a major role in the smart home security. Reactive steps has to be taken based on the strength of integrity of the data received from the nodes in the network to achieve automation. In proposed method, nodes calculate the Message Authentication Code (MAC) through AES-CBC technique and send MAC along with the message. Controller on receiving the

packets, calculates the Message Authentication Code on message and compare it with the received MAC. Malicious node which tries to change the message can be easily caught, as it cannot calculate the same MAC with different key.

5.4.4 Resilience

Resilience is an important security concern. Despite strong security mechanisms, nodes are susceptible for attacks. When a node is compromised by attacker, it is very important to ensure security with rest of the network. Unlike, Z-wave [16] and ZigBee [18],[22] protocols, the nodes in proposed scheme will not contain the keys of every other node. If any node is compromised in either Z-wave [16] or ZigBee [18],[22], as it contains keys of all other nodes in the network, all the keys are exposed. In proposed scheme, when a node is compromised, only key of corresponding node is exposed.

CHAPTER 6:

ANALYSIS OF PROPOSED SCHEME

Secure smart home scheme is derived from existing schemes. Proposed scheme do not contradict any of existing protocols. Existing protocols, already had proved their mark in the smart home industry. Proposed scheme is an integration of existing techniques, to provide better security in the smart home. We provide attack- defense model for the AES-CBC-CTR encryption mode, we adapt to achieve confidentiality of data.

6.1 Security Against AES-CBC-CTR

Advanced Encryption Standard is the secure standard till date in symmetric cryptography. AES in its original form is still possible to crack by brute-force attack. A better security can be achieved using it in combination of CBC mode and CTR mode. This mode is already in practice in ZigBee [18],[22] protocol. CBC mode is used to calculate the MAC of data, so as to provide integrity. Data and MAC calculated on data are then encrypted with AES using CTR mode to provide confidentiality. Proposed scheme on using these efficient modes on AES can defend against attacks like Cipher-text only attacks, Known Plaintext attacks. Analysis of proposed scheme is based on assumption that key is not compromised.

6.1.1 Cipher-Text Only Attacks

6.1.1.1 Attack

Attacker can eavesdrop the communication to get the cipher-text. Strong Cryptanalysis on these cipher-texts can provide knowledge of secret key.

6.1.1.2 Defense

AES-CTR mode is used to encrypt the data in proposed method. AES-CTR is a stream cipher. A nonce, which is a counter is encrypted with the key derived from accelerometer fingerprinting results in a bit sequence, which is further used to encrypt the data. Despite strong cryptanalysis, attacker cannot calculate the bit sequence in which the plain-text is encrypted, because this bit sequence is generated by encrypting a nonce with a highly random key.

6.1.2 Known Plain-Text Attacks

6.1.2.1 Attack

Known Plaintext attack are very common in smart home. In smart home environment malicious node can sense the same parameter as legitimate node. Attacker knows the plaintext. Attacker can also eavesdrop the communication to retrieve cipher-text. Attacker can perform cryptanalysis on plain-text and cipher-text pairs to get information about key.

6.1.2.2 Defense

Despite having knowledge of plain-text and cipher-text, attacker cannot get the key of device. Attacker might get the bit sequence, with which the plaintext is encrypted, as encryption is XOR operation between the plaintext and derived bit sequence. Attacker cannot derive any information of key with the information he has.

6.2 Security of Wireless Sensor Network (WSN) in Smart Home Automation

6.2.1 Replay Attack

Replay attacks on Wireless Sensor Network (WSN) are very common. Attacker intention on launching replay is to discharge the battery of sensors. Replay attacks can be serious threat to the availability of service. Malicious node can impersonate either the controller or any sensing device. Controller being computationally more complex than sensing node, can withstand this attacks. On the other hand, impersonating controller and sending the data seamlessly would discharge the battery of sensing node.

6.2.2 Defense

Replay attacks can be easily defended by using CTR mode of AES. Key of AES in CTR mode is generated from a nonce, which typically is a counter. Counter in CTR mode of AES increments by 1 for every communication. Counter is set to random Initialization vector and is communicated with controller. For every communication, sensor node increments this counter and generate bit sequence, which is further used for encryption. Symmetrically, controller will also increment the value of Initialization vector and derives key bit sequence to decrypt the cipher text. Attacker who has cipher text instance of communication, tries to send the same packet to sensor nodes, impersonating the controller. However, sensor nodes can easily detect this and drops the packet that is sent by attacker.

CHAPTER 7:

COMPARATIVE ANALYSIS OF PROPOSED SCHEME

Proposed method do not contradict or oppose any of the existing schemes. Instead, had integrated best practices from all the existing schemes. Our major concern is to provide a secure communication across different smart home devices. Smart home providers either proprietary or open source has provided partial automation of smart home. Proposed method by using accelerometer fingerprinting, can cut the barriers in policy making by smart home providers. Proposed method, which is derived from existing techniques, can motivate the smart home providers to extend their services to achieve complete automation. This section provides complete comparative analysis of proposed method with existing techniques.

7.1 Accelerometer Fingerprinting v/s Pseudo Random Number

Despite strong Pseudo Random Number Generator algorithms to generate a bit sequence, to identify any device uniquely, the trust on the randomness is not so motivating. Tiny Encryption Algorithm [24],[25],[26] which uses Pseudo Random Number Generator for keys, had decreased the effective length of key from 128-bit to 126-bits [24]. To overcome this problem and to ensure complete randomness, proposed method rely on manufacturing errors, which are completely random. Despite, of fact that not all smart devices are equipped with accelerometer fingerprinting, we believe accelerometer fingerprinting would be off the shelf technology to identify devices uniquely.

7.2 Centralized Approach v/s Distributed Approach

Centralized approach is defined as centralized control over communication. Centralized node (controller) in smart home provides communication interface between all the smart devices. Z-wave [16] technology is an example for centralized approach. ZigBee [18],[22] which is distributed approach, but can also operate through centralized approach.

Distributed approach is defined as decentralized control over communication. Every smart device will be able to communicate with every other smart device in the communication range. Every device is connected to internet and can send the data to client location for behavioral analysis of user. Client which offers this smart home service would send recommendation to user to make user life smart. ZigBee [18],[22] in its naive form is an example for distributed approach.

Both approaches have advantages and short-comes, as far as secure smart home is concerned. Traits to analyze above mentioned approaches are; Resilience, Connectivity, Storage Complexity.

7.2.1 Resilience

Despite, strong security mechanisms that are employed in smart home, when a smart device is compromised, distributed approach discussed above would reveal the keys of every other smart device in smart home. Whereas, in proposed scheme, with centralized approach, when a smart device is compromised, only key of corresponding smart device is only exposed. ZigBee [18],[22], despite using both the approaches, fails to provide resilience.

7.2.2 Connectivity

In distributed approach, as every device is in possession of keys of every other device, strong connectivity between the devices is expected. On flip side, in centralized approach, as every node has to communicate with the centralized node, will provide an illusion of low connectivity.

However, using mesh network topology, proposed scheme will ensure good connectivity. Despite the fact that all the devices can share data with centralized controller, these data packet traverse in the same as in distributed approach, with the help of intermediate nodes. However, intermediate nodes which do not possess the keys of source device, cannot decrypt the packet. Once the packet reaches controller, controller can decrypt the packet to retrieve data. This way we ensure complete resilience, by preserving connectivity.

On careful observation, not every device in smart home communicates with every other device. For instance, security system which provide door lock, will never communicate with temperature sensors inside smart home. This fact reduces the communication complexity in smart home and also provides the motivation for centralized approach.

7.2.3 Storage Overhead

Sensors in smart home are expected to have very less storage resources. As the number of smart devices increases with time, storage complexity of device in distributed approach would be a bottleneck. In centralized approach as every device is expected to communicate only with the controller, this complexity is mitigated to centralized node. Centralized node being high capable can store the keys of all the devices in smart home.

CHAPTER 8:

CONCLUSION

Smart home technologies are being revolutionized over few years. Market, started with a simple automated locks and is extended to provide best living experience for user by behavioral analysis. Existing technologies had already marked their significance in providing security to the smart home. However, approaches that existing technologies follow, can be improved. Proposed method would solve some of the issues with existing technologies. Proposed method do not contradict with existing techniques, instead compliment them by taking the efficient schemes they implement.

On solving the problem of identifying the devices, we replace Pseudo Random Number Generators (PRNG) with True Random Number Generator (TRNG), the accelerometer fingerprinting. Unlike existing technologies, proposed method can be extended to the smart devices from different manufacturers. Proposed method still stick to basic mesh topology, used by most of the existing technologies. Proposed method implements the centralized approach for communication. Centralized approach provides high resilience compared to distributed approach. In approach of providing confidentiality, message authentication and integrity of data, we implement secure AES-CCM encryption scheme, similar to ZigBee. Despite, using same encryption technique as ZigBee, we provide better resilience and robust defense for replay attacks. This thesis provides complete analysis of proposed scheme.

CHAPTER 9:

FUTURE WORK

Smart Home technology aims to provide better living experience by achieving automation, and also by behavioral analytics. This thesis primarily focusses on automation of devices that communicate over Wireless Sensor Networks. Future work on this technology can focus on unique security mechanism to all the different networks that are available in smart home, to achieve better automation. Future work can also focus on the variety of integration protocols that act on the data received by controller from smart devices. Controller, being in possession of all the secret information of smart devices in smart home is more susceptible for attacks, future work might focus on securing the controller node. It is also important to secure the inbound and outbound data traffic of smart home. Future work can focus on making strong decision taking algorithms, which makes the tradeoff between the data received from sensors in smart home and data received from the cloud, which computes behavioral analytics. Despite, random key generation mechanism in proposed scheme, we had not discussed the efficient way of key exchange between the smart devices and controller. Future work can contribute for secure key exchange mechanisms in smart home.

REFERENCES

[1] Khan, Faraz. "Future scope and possibilities in Internet of Things." In*International Conference on Advances in Engineering Science and Management*, vol. 310. 2015.

[2] https://www.youtube.com/watch?v=_AlcRoqS65E

[3] https://www.youtube.com/watch?v=QaTIt1C5R-M

[4] Schreiber, Arye. "Through the looking GLΛSS: Google Glass™, privacy, and opacity, with an Israeli law twist." *International Data Privacy Law* (2014): ipt034.

[5] https://developer.apple.com/library/ios/documentation/UIKit/Reference/UIDevice_Class/index.html

[6] Sweeney, Latanya. "My phone at your service."

[7] Blog, Android Developers. "Identifying App Installations." (2011).

[8] Developer, Android. "Media Player http://developer. android. com/reference/android/media." *MediaPlayer. html Diakses* 1 (2013).

[9] Bojinov, Hristo, Yan Michalevsky, Gabi Nakibly, and Dan Boneh. "Mobile device identification via sensor fingerprinting." *arXiv preprint arXiv:1408.1416*(2014).

[10] Mendes, Tiago DP, Radu Godina, Eduardo MG Rodrigues, João CO Matias, and João PS Catalão. "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources." *Energies* 8, no. 7 (2015): 7279-7311.

[11] Kanth, V. Rama, K. Aditya Kumar, and K. Keerthana. "A Survey on Bit keys in Cryptography."

[12] Daemen, Joan; Rijmen, Vincent (March 9, 2003). "AES Proposal: Rijndael"(PDF). National Institute of Standards and Technology. p. 1. Retrieved 21 February2013.

[13] Von Neumann, John. "13. Various Techniques Used in Connection With Random Digits." (1951).

[14] http://www.calpoly.edu/~gthorncr/ME302/documents/AccuracyofGravity.pdf

[15] http://www.memsjournal.com/2010/12/motion-sensing-in-the-iphone-4-mems accelerometer.html

[16] “Smarten up your dumb house with Z-Wave automation”

[17] "ONE-NET wireless control for everyone. • • About ONE-NET • •

[18] Gislason, Drew. *ZigBee wireless networking*. Newnes, 2008.

[19] G. Derene, “How to Control Your Home with your Cell Phone,” online, http://www.popularmechanics.com/home/improvement/4301977, 2009.

[20] Darbee, Paul. "INSTEON The Details, Smarthouse." *Inc., Aug* 11 (2005): 68.

[21] "Understanding Z-Wave Networks, Nodes & Devices". Vesternet.com. Retrieved2012-11-19.

[22] http://www.libelium.com/security-802-15-4-zigbee

[23] Fouladi, Behrang, and Sahand Ghanoun. "Security evaluation of the Z-Wave wireless protocol." *Black hat USA* 24 (2013).

[24] Kelsey, John, Bruce Schneier, and David Wagner. "Related-key cryptanalysis of 3-way, biham-des, cast, des-x, newdes, rc2, and tea." *Information and Communications Security* (1997): 233-246.

[25] Kelsey, John, Bruce Schneier, and David Wagner. "Key-schedule cryptanalysis of idea, g-des, gost, safer, and triple-des." In *Advances in Cryptology—CRYPTO'96*, pp. 237-251. Springer Berlin Heidelberg, 1996.

[26] Steil, M. "Mistakes Microsoft Made in the Xbox Security System. Chaos Communication Congress (2005)." (17).

[27] Needham, Roger M., and David J. Wheeler. "Tea extensions." *Report, Cambridge University, Cambridge, UK (October 1997)* (1997).

[28] Shipley, Peter. "Insteon: False Security and Deceptive Documentation"