www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-5, Issue-2, May 2017
Review Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

CSI Based Key Generation Technique

S.G. Kamble[1*], K.T. Jadhao[2]

[1]Dept. of ETE, Alamuri Ratnamala Institute of Engineering and Technology (ARIET), Thane, India
[2]Dept. of ETE, Alamuri Ratnamala Institute of Engineering and Technology (ARIET), Thane, India

Corresponding Author: kamble.sandeep1990@gmail.com

Received 06th Feb 2017, Revised 20th Feb 2017, Accepted 12th Mar 2017, Online 30th May 2017

***Abstract*—**The role of communication in wireless technology is very important. This communication needs to be secured. System Administration has a number of aspects of which network security is considered as very essential. We live in a world where various types of information such as voice, multimedia or data analytics can be easily accessed anywhere and at any time. So we need to make sure that information is highly secured, authentic and accessible only to the authorized user. The user must receive this information with the highest level of security. We can secure communication by various techniques such as RSS. However it has its own demerits. To overcome its issues we can use key generation techniques based on CSI information in M2M communications. For that we will use OFDM channels. The process of generating a key using CSI information can be more efficient in terms of providing security as compared to RSS based technique, as they can generate a longer key. This technique generates the key randomly thereby preventing the attacker from decoding the key within the time span during which it would be vulnerable to the communication. The CSI information of the OFDM channel has a property by which it prevents an attacker from using the same algorithm and trying to sabotage the communication, by generating a different key.

***Keywords*—**M2M(Machine to Machine), CSI (Channel State information), OFDM(Orthogonal Frequency Division Multiplexing), RSS(Radio Subsystem)

I. INTRODUCTION

In today's world, an important aspect of communication and technology is security. Wars are being fought in the virtual world rather than in the real world. Wars are being fought by attacking the data and information of the enemy rather than with arms and ammunition. There is a rapid increase in cyber warfare. So to ensure the integrity of the system there is a need to build a secure data system. Communication between two devices must be done only in a secure environment. So we explore the security aspect for M2M communication of IoT. In wireless communication securing information can be a very challenging task. Security has become even more challenging due to the inclusion of both dynamic and static devices in M2M Communication. If we consider network security, it would be better if the M2M devices are small, compact, low power consuming and work efficiently. Thus we use CSI based key generation technique. *Channel State Information (CSI)* contains information about parameters concerning the channel and the interference. This information is extracted from the feedback channel from the receiver.[3]Orthogonal Frequency Division Multiplexing (OFDM) based modulation contains the subcarrier which is highly uncorrelated. In OFDM bandwidth is divided into various channels. All the subcarriers maintain orthogonally between each of them. Each subcarrier should experience only flat fading and hence these are narrow in nature. Thus there is very less chance of ISI occurring. Each subcarrier contains the CSI information within the channel[1-4]. This property of uncorrelated channel will be used to extract the key from CSI information. There are some physical properties of the channel in the wireless form of communication. One of the parameters of the channel which provides information available in the channel is CSI. There can be different CSI for the transmitter and the receiver respectively viz. CSIT will be different from CSIR. The information available at the transmitter end is the CSIT and the information available at the receiver end is CSIR. There are two levels of CSI defined, namely statistical channel state information, also known as long term CSI and instantaneous channel state information, also known as short term CSI. The current channel condition is known by the short term CSI, which portrays the filter response. Thus on knowing the filter response, the received signal can be optimized to achieve low bit error rates. Long term CSI knows the statistical characteristics of the channel. The limitations of CSI information are dependent on the changes in channel conditions. Only long term CSI should be used in the systems where channel conditions changes very fast. Similarly, short term CSI should be used in the systems where channel conditions vary at a lower rate. Our system should use the combination of both of these CSI information's [5-7].

Let us take an example of Alice and Bob, to understand in depth about how the key will be generated using the CSI information. A random signal will be sent to each other by Alice and Bob through the subcarrier of OFDM channel. Each subcarrier contains CSI information in it. Since Alice and Bob are at the same distance while sending the

© 2017, IJSRNSC All Rights Reserved

information, CSI information will be same. We assume that the condition remains same while exchanging the random signal. We use the same CSI to generate a key which will be private only to Alice and Bob. If Eve, the attacker, tries to intercept the signal, it will not be possible as Eve will be λ/2 distance apart and so she cannot deco relate the information. It is not possible with RSS because it suffers from a low key generation rate, it is easier to inject its information.

II. LITERATURE SURVEY

CSI information is extremely useful at the receiver as it needs to know the channel for accurate power control, scheduling, and data demodulation. The base station transmits and receives on different frequencies and so Frequency-division duplex (FDD) systems are more difficult. Therefore the received pilot cannot be used to infer anything about the multi-antenna transmit channel. However, the time occupied in frequency-duplex CSI transfer is generally less than one might expect and falls as the number of antennas increases. Thus, burden of learning this information at the base station paradoxically decreases because the total amount of channel information increases with the number of antennas at the base station. Thus, the advantages of having more antennas at the base station extend from having network gains to learning the channel information. The author says that the timely possession of CSI is a key enabler in multiuser communication. The transmitter contains an array of antennas since MIMO systems are used these days. A transmitter array can send multiple messages simultaneously with CSI. The author explains how TDD system offers a simple way to acquire CSI information and how it becomes difficult in the case of FDD systems. The key generation protocol requires that we make an assumption that a sufficiently distant adversary is unable to guess a generated secret due to the unpredictable behavior of multipath signal propagation. The broadcast nature of the channel can be used to inject some bits while the channel estimation of Alice and Bob is further used by them as a part of their secret key. In this technique the bits are injected at specific interval and hence the protocol is not disturbed and the bits are injected. In key generation technique, there are three phases i.e. Quantization phase, Information reconciliation phase and key verification phase. In quantization phase, the channel response is estimated by the channel information such as RSS and CIR. Based on the channel response that is obtained, a bit stream is generated which will be almost the same for Alice and Bob. In Information reconciliation phase, the quantized information is reconciled by some error correcting codes. This is done because the channel estimate information varies due the effect of noise. Finally, both Alice and Bob have to agree with the generated key. In the key verification phase the secret key generated is verified by both the parties.

Assume that the attacker is not violating any constraints on the physical distance, such as being near legitimate transmitters. The distance between the attacker and the legitimate nodes is comparably small. The attacker is always in line of sight of both Alice and Bob. Aim of the attacker is to destroy legitimate packets sent by Alice and Bob when required.

The key generation rate of RSS was very low and so a technique is needed in which the key generation rate can be increased. This can be done by exploring using multiple frequencies, exploiting spatial and temporal variation of a radio channel. The use of RSS based technique provides only a single RSS value over a wireless packet *(coarse-grained information)*, hence there is a limitation using RSS based technique even with help of a variety of quantization. So we can use OFDM channels. It has multiple sub carriers. Some CSI information is contained by each sub carrier. Thus OFDM provides a detailed CSI which can be used to obtain a high key generation rate and hence make key generation from physical parameters more practical. We define the problem statement to justify our aim and objective. We want to generate a key from CSI information available in OFDM channel. [5] To make it difficult for a malicious user to detect it, the generated key should be random. Thus we can provide high level security for the communication. The key should be generated fast compared to RSSI based key generation, as the communication can be faster in M2M devices. The malicious user should not have any possibility of key recovery and any opportunity for sabotage as was done in the previous research. Key generation should be efficient and the key should be able to be generated without external hardware. [8]

III. MOTIVATION

Communication has advanced pretty forward from speed and quality. Now, it is the era of automation. Till today there was human intervention in using a machine, but now as we proceed in the next generation there is a need for machine to be smart and intelligent. Artificial Intelligence forms one part of automation but major portion remains in making the machine smart enough so that it can communicate by itself. Hence the invention of Machine to Machine (M2M) Communication evolves.

Further, as we go into the details of the security aspect of M2M communication, we find that the devices within M2M communication will be small and compact. Since it is said that there will be around 50 billion devices that will talk to each other without intervention of human being. A device can be as small as a pen drive and can be fitted in our shoes for our positioning purpose. The communication that happens between the two devices needs to be authorized, authentic and secured. Hence in order to design a secured communication, we need a secret key that can be used to encode the data in order to be prevented from phishing. As mentioned earlier, the devices within M2M communication will be very small. So an additional hardware cannot be implemented for the generation of the key. So there is a need to generate a secret key with the existing information available. This key should not be

© 2017, IJSRNSC All Rights Reserved

shared as the wireless channel remains vulnerable to attack. So the key should be generated by both the communicating devices.

As the need for internet increases and connected networks expands, network security has become a major and critical factor to be considered [3]. One can decrease the chance of spoofing, identity or information theft by increasing network security. A big concern to the major enterprises today is piracy. Many software, books, movies, music are stolen by malicious user, thus breaching the security [3]. As number of hacker tools has come up, more people started destroying the secured world. Many of the individuals today are skilled in hacking and breach others privacy in several ways. These kinds of people have developed in recent years. High level programming skill is not the prerequisite for a hacker today, many open source tools are available on internet for that. Attacker passes through several stages to successfully carry out an attack. Thus Security has become a greater source of motivation in developing this algorithm. Also, the security standards for M2M are not finalized by the standard bodies which give enough motivation for the development of this algorithm [3]. It gives an opportunity to research and develop something which is not available.

Earlier research shows that RSSI (Received signal strength Indicator) value can be used for generation of the key. This method was useful in eliminating the extra hardware required for key generation. But it had its own disadvantages. The key generation rate was very slow. As the research advanced, people found out that CSI information within an OFDM channel can be used for key generation. But the earlier research had its disadvantage. If the third party could find out the specific instances where attack opportunities were possible, then the algorithm could be broken. This encouraged us to design an algorithm such that CSI information of the available OFDM channel will be used and the attacker is not able to break the algorithm.
Thus we design an algorithm considering all the previous research and the problems associated with it. And we come up with our solution towards the security aspect of M2M communication.

IV. PROPOSED SYSTEM

M2M communication is often used for exchanging information. It is an important aspect of warehouse management, remote control, robotics, traffic control, logistic services, supply chain management, fleet management and telemedicine. Key components of an M2M system include sensors, RFID, a Wi-Fi or cellular communications link and autonomic computing software programmed to help a networked device interpret data and make decisions. Security being major concern for this technology, we find out that the best of research have some shortcomings and drawbacks. Thus it provides motivation for us to explore the security aspect and come up with a better solution. In order to generate key in CSI based algorithm we can use *E-KET (Enhanced – Key Extraction Technique).*
The main *features* of the E-KET are as follows,

1. Minimization of bit injection opportunities hence eliminating sabotaging attack.
2. Significant reduction in Key recovery opportunity resulting into better security aspects
3. Efficient in terms of time and hence can be used for M2M communications where fast key generation is utmost important.
4. Provides solution to the problems associated with previous research based on RSS and CSI based key generation.
5. Predictability of the key bits very low as the concept of interleave matrix is applied.

Our implementation contains three Devices A and B the authentic devices who want to communicate with each other. These devices are Alice and Bob as we name them for our convention. Device C, stated as Eve, tries to listen to device A and B and try to find out the key so that he can break the algorithm in order to listen the communication between them. The communication channels formed between the three are different from one another.

The device C which is not the authentic device in the communication tries to listen to both devices A and B. Thus there are various options for device C to destroy the communication. He can find out the key by listening or he can use sabotaging opportunities to add his own information in the channel between devices A and B or he can try to destroy the key generated by device A and B.
E-KET is deployed in each device, but it is specific to its CSI value. Thus when Device C tries to gather the information from Device A and B, it will be difficult for Device C to find out the key between the two. The algorithm may be same in all the device, but the key that will be generated based on CSI value will be authentic only between Device A and B. Thus it will be difficult for Device C to know the key and break the communication. The randomness is maintained by E-KET which ensures that the key is not easily decodable. Thus, our system consisting of three devices will deploy E-KET as a solution to the problem statement.

E-KET is deployed in each device, but it is specific to its CSI value. Thus when Device C tries to gather the information from Device A and B, it will be difficult for Device C to find out the key between the two.

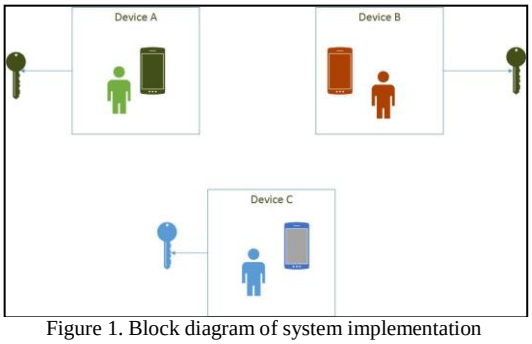

Figure 1. Block diagram of system implementation

© 2017, IJSRNSC All Rights Reserved

The algorithm may be same in all the device, but the key that will be generated based on CSI value will be authentic only between Device A and B. Thus it will be difficult for Device C to know the key and break the communication. The randomness is maintained by E-KET which ensures that the key is not easily decodable.

V. CONCLUSION

Security is a major concern for M2M communication as this is the latest form technology. Standardizing the security protocol remains the key consideration. Our work towards this standardization is a motivation from the drawback obtained from the previous research. We found out in the previous research that RSS based key generation technique was very slow. And designing a security scheme for M2M communication which will connect billions of devices had to be fast. So we went through various aspect of the research and found out that there is a CSI based key generation technique which is fast compared to RSS based key generation technique. Using CSI based technique was found to be beneficial as it does not require additional external physical hardware for key generation and also it proved to be very fast.

Further we found out that the latest research related to key generation using CSI based approach had some drawback. There were bit injection opportunities for the malicious user which can compromise the security of the communication system. Thus we researched and found out a technique called E-KET. E-KET is an algorithm which defines a procedure and provides high level of security. It overcomes the drawbacks observed by previous research to a great extent. The drawback of previous research was sabotaging attack and key recovery opportunity. E- KET eliminated the possibility of sabotaging attack and significantly reduced the key recovery opportunities. Thus E-KET is proved to be fast enough as compared to RSS based technique which is practically used. E-KET was implemented in MATLAB due to the advantage of its physical channel parameter. MATLAB has a communication toolbox which has a function to calculate the CSI value of the OFDM channel. Also, we used MATLAB functions to find the time taken by E-KET to execute the algorithm. Thus we find the efficiency in terms of the time parameter.

REFERENCES

[1] Meng Zhang, Yuan Liu, and Rui Zhang, "*Artificial Noise Aided Secrecy Information and Power Transfer in OFDMA Systems*", *IEEE Transactions on Wireless Communications* Vol. 15, No. 4, pp. 3085 – 3096, 2016.

[2] S. Tamilarasan, P. Kumar, "*A Survey on Dynamic Resource Allocation in MIMO Heterogeneous Cognitive Radio Networks based on Priority Scheduling*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.1, pp.53-59, 2017.

[3] Rizwan Ahmed malik, Shahid Shabir, Ruchi Singla, "*Review on OFDM: Concept, scope and its application*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.8, pp.48-50, 2016.

[4] Chih-Yao Wu, Pang-Chang Lan, Ping-Cheng Yeh, Chia-Han Lee; Chen-Mou Cheng, "*Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices*", IEEE Journal on Selected Areas in Communications, Vol. 31, No. 9, pp. 1687-1700, 2013.

[5] B. Benarji, GS. Rao, SP. Setty, "*BER Performance of OFDM System with various OFDM frames in AWGN, Rayleigh and Rician Fading Channel*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.4, pp.6-11, 2015.

[6] Y. Liu, S. C. Draper, and A. M. Sayeed, "*Exploiting channel diversity in secret key generation from multipath fading randomness*", IEEE Transaction on Information Forensics and Security, Vol. 7, No. 5, pp. 1484–1497, 2012.

[7] X. Wang, M. Tao, J. Mo, and Y. Xu, "*Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks*", IEEE Transaction on Information Forensics and Security, Vol. 6, No. 3, pp. 693–702, 2011.

[8] Y. Liu, S. C. Draper, and A. M. Sayeed, "*Exploiting channel diversity in secret key generation from multipath fading randomness*", IEEE Transaction on Information Forensics and Security, Vol. 7, No. 5, pp. 1484–1497, 2012.

© 2017, IJSRNSC All Rights Reserved