INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue5)
Available online at www.ijariit.com

OFDM Based Key Generation Technique

Sandeep Kamble
Alamuri Ratnamala Institute of Engineering and Technology (ARIET) Thane- Maharashtra
kamble.sandeep1990@gmail.com

Kailash T. Jadhao
Alamuri Ratnamala Institute of Engineering and Technology (ARIET) Thane- Maharashtra
Maharashtraktjadhao@gmail.com

Abstract: ***With enhancement in wireless technology, security has become an important part in designing of the network. Network security is an important aspect of system administration. We are living in a world where there is access to information anywhere, anytime, be it voice, multimedia or data analytics. This information should be provided to the user with the highest possible security. Thus the information exchanged for communication should be highly secured, authentic and only accessible to the authorized user.***

Recent research has shown that this security can be provided through RSS (Received Signal Strength) based key generation techniques for authentication of the user. But RSS based key generation technique has a drawback that the key generation rate is very low. Also, RSS based technique is highly applicable for mobile devices. In M2M Communication the devices can be static or mobile based. So we explore a technic which is based on Key generation through CSI (Channel State Information) of a channel. Key generation using CSI information can be efficient in the terms of providing security as they can generate quite a long key as compared to RSS based technique.

We deploy an algorithm as a solution to key generation without using additional hardware for key generation and verify that the malicious user is not able to decode the key sighting to the randomness obtained to our algorithm. The major portion of the algorithm concentrates on making the key random so that the attacker is not able to decode the key within a time span which is vulnerable to the communication. When an attacker tries to use the same algorithm and try to sabotage the communication, due to the property of CSI information of OFDM channel, the generated key will be different. Thus it will not match with the secret key used for actual communication. Hence the user will not be able to hijack the communication.

Keywords: CSI, RSS, M_2M, OFDM, Network Security.

[1] INTRODUCTION

Security is an important aspect in today's world. The wars have shifted its course to cyber wars rather than actual wars. Wars are not fought with arms, ammunition, and artillery, but with attacks on the enemy's data. Cyber Warfare has increased in today's world. Thus there arises a need of building a secure data system to ensure the integrity to the system. Whenever there is communication between two devices, it has to be secured one. Thus we explore the security aspect for M2M communication of *IoT.*

Due to shared nature of channels in wireless communication, securing the information is a challenge. With the inclusion of both dynamic and static devices in M2M Communication, security has become even more challenging. Research in the field of key generation techniques has portrayed that RSS based key generation is vulnerable to low secret bit generation rate due to coarse-grained channel information. Also, since the M2M devices work on 6LoWPAN protocol, separate key generation module cannot be embedded in these devices [1]. M2M devices will be small, compact, low power consuming and will have to work efficiently considering the network security. Thus we explore a key generation technique based on CSI information of a channel. *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.

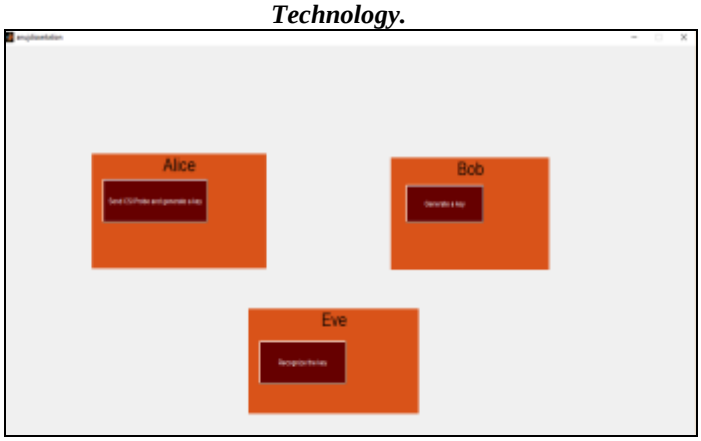

Figure: 1. GUI for simulation of KET

[2] CONTRIBUTION

As we see that there is a lot of motivation in the creation of a Secret key without actually exchanging the key on a public channel, we propose our solution in the form of an algorithm. We see that a secret key can be generated using CSI information of the OFDM channel without the need to have an external hardware for key generation. Some research shows that the previous CSI based key generation technique can be broken by Sabotaging and Key recovery opportunities. Research says that if a third party (Eve) tries to inject her information during generation of the key, she will not able to control the reception of a signal at both the legitimate entities and thus the attack can be identified immediately. The general idea of the attacker is to attack the channel between legitimate users during Quantization phase. In order to avoid the detection of a phishing attack, Eve waits for opportunities to inject her bits in the communication between the two legitimate users that help her to keep the key generation protocol intact and still succeed [4]. Thus to overcome this drawback in the previous research, we design an algorithm named E-KET which will generate a key based on CSI information of the OFDM channel. This key will maintain its randomness and eliminate the chances of Key recovery opportunity.

[3] PROBLEM DEFINITION

Recently, physical channel information has attracted the wireless devices to a greater extent. The main idea of using a physical channel information is to utilize the temporal and spatial randomness of the wireless channel to extract a secret key that can be used on a public channel. Traditional cryptography based method relies on the *computational hardware*. In a wireless channel, there is a scope to explore the physical property, as the channel is highly uncorrelated with each other. Thus we can use physical channel based secret key generation method rather than the traditional ones. This will be proved helpful as the devices will be small, compact, limited resource-based and lack key management infrastructures. Currently, each device sends a signal strength indication to the serving stations known as Received Signal Strength Indication (RSSI). This information is used in the existing systems today. It was found that the key generation rate is very low. Hence there is a need for a technique in which key generation rate is increased to a great extent. This can be done by exploring using multiple frequencies, exploiting spatial and temporal variation of a radio channel. Using RSS based technique provides only single RSS value over a wireless packet *(coarse-grained information)*, there is a limitation using RSS based technique actually even with help of variety of quantization. Coarse-grained approach proves to have some shortcomings so we explore *fine-grained physical layer details* available in OFDM (Orthogonal Frequency Division Multiplexing) signal. OFDM signal has multiple sub carriers. Each sub carrier contains some CSI information. Thus OFDM provides detailed CSI which can be used to obtain high key generation rate and hence make key generation from physical parameters more practical.

ALGORITHM OF PROPOSED SYSTEM

1. Alice and Bob exchange their CSI information which can be obtained from the uplink channel of OFDM signal. This information is a random signal and is analogue in nature. Sa is the information available with Alice and Sb is the information available with Bob.
2. Sample Sa and Sb with a common sampling rate for both Alice and Bob. We get the values in the form of the array after sampling Sa and Sb. Thus Sa and Sb are now the arrays of values.
3. Calculate the threshold values q+ and q- at both Alice and Bob independently.
   $q+ = \mu(\text{samples of Sx}) + \alpha * \sigma(\text{samples of Sx})$ [From eq1]
   $q- = \mu(\text{samples of Sx}) - \alpha * \sigma(\text{samples of Sx})$ [From eq2]
   Where μ is the mean of all the samples, σ is the standard deviation of all the samples and α is a constant to differentiate the values of q+ and q-. Generally, α is set to 0.3 - 0.45.

4. Discard all the values in between q+ and q-. The values above q+ will be assigned value 1 while the values below q- will be assigned value 0. Thus we get a stream of values at both Alice and Bob. This stream of values is termed as Ba and Bb.
5. Check if the number of bits in Ba and Bb respectively is minimum 10 bits. If yes proceed to 6. Else go to 1.
6. Calculate the number of bits in Ba and Bb respectively. Define a counter. Initialise the counter with the value equal to the first bit of the number calculated.
7. Define an interleaving matrix of size m X n.
8. Check the number of bits in Ba and Bb respectively. If a number of bits in Ba and Bb respectively is less than m*n go to 9. Else go to 10.
9. Zero pad Ba and Bb respectively such that the number of bits in Ba and Bb is equal to m*n. go to 11.
10. Discard the values that exceed m*n. Go to 11.
11. Insert the values of Ba and Bb row-wise in the defined interleave matrix. And retrieve column-wise. And update this values respectively in Ba and Bb. Decrement the counter.
12. Check if the counter is 0. If it is 0 stop the algorithm else go to 11.

[4.1] PERFORMANCE EVOLUTION

The figure shows the key generation rate for Alice with different key sizes. Thus we can see from figure 8 that the average key generation rate for Alice is 1425.2916 bps. The X-Axis displays the key generation rate while the Y-Axis shows the different key sizes. This is based on the timing functions in MATLAB. We consider the average of all the values for different key sizes. Thus the average for Alice is 1425.2916 bps which is very good as compared to the RSS based key generation.

On a similar basis, we find out the key generation rate provided by Bob. The KGR may vary depending on the time taken by each individual to identify the bits and process them to obtain the final key. Figure 9 shows the key generation rate of Bob. Thus, as seen from figure 9 the average key generation rate for bob is higher than Alice. The average key generation rate is 1751.8448 bps.

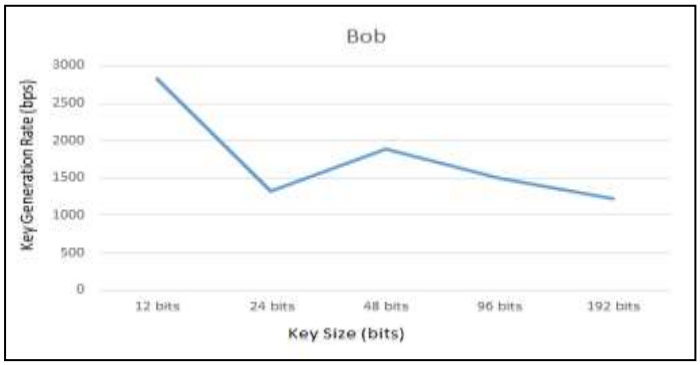

Figure 2. Key Generation Rate of Alice

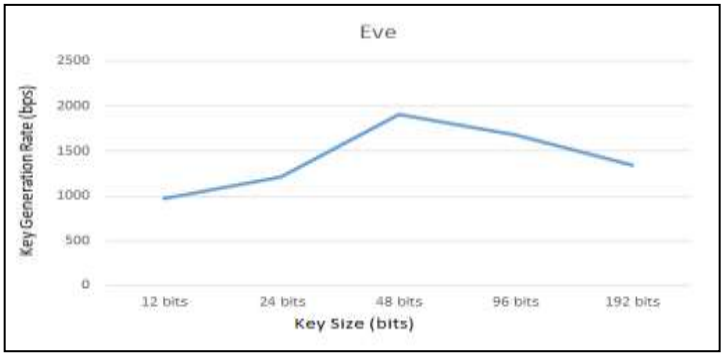

Figure: 3. Key Generation Rate of Bob

As seen from figure 9, the KGR for the 12-bit key is higher and it eventually decreases with a 192-bit key. The pattern for KGR is not fixed to make the simulation random. This also ensures the randomness of E-KET. This is the simulation result and may vary as per the computing speed of the test bed. Also, the bits obtained by different entities

are different and hence the processing time taken differs. This makes the KGR vary with respect to different entities. Though the bits obtained by Alice and Eve remains the same, the KGR of both Alice and Bob varies as they are two different entities. KGR is the important parameter to evaluate the performance of E-KET. We need to evaluate the KGR of Alice, Bob and Eve and compare them with the RSSI based key generation technique. Thus we are able to analyse the KGR to draw a conclusion that the CSI based key generation technique is better than RSSI based key generation technique.

[6] 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 aspects 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.

[7] ACKNOWLEDGEMENT

It is a great pleasure and a moment of immense satisfaction for me to express my profound gratitude to my project guide Prof. K.T. Jadhao, Assistant Professor, Electronics and Telecommunication Engineering Department whose constant encouragement enabled me to work enthusiastically. His perpetual motivation, patience, and expertise in discussion during the progress of work have benefited me to an extent, which is beyond expression. Working under his guidance has been a fruitful and unforgettable experience. Despite his busy schedule, he was always available to give me advice, support, and guidance during an entire period of my project. The completion of this project would not have been possible without his constant support and patient guidance.

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, January 2016, pp. 3085 – 3096.

[2] Yang Zhao, Xiangyang Wang, XiaotengGu, Wangtao Wan and Qiao Pang, "Training Sequence Design for Channel State Information Acquisition in Massive MIMO Systems". *Proceedings of 2015 IEEE International* Symposium *on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, September 2015, pp. 1712 – 1716.

[3] Xiaohua Wu; Yuexing Peng; Chunjing Hu; Hui Zhao and Lei Shu. "A Secret Key Generation Method Based on CSI in OFDM-FDD System," *Proceedings of 2013 International Conference on IEEE Globecom Workshops (GC Wkshps)*, December 2013, pp. 1297 – 1302.

[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, August 2013, pp. 1687 – 1700.

[5] Junqing Zhang; Alan Marshall; Roger Woods and Trung Q. Duong. "Secure Key Generation from OFDM Subcarriers' Channel Responses", *Proceedings of 2014 International Conference on IEEE Globecom Workshops (GC Wkshps)*, December 2014, pp. 1302 – 1307.

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

[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 Transactions on Information Forensics and Security*, Vol. 6, No. 3, September 2011, pp. 693–702.

