iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1480

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Enhanced Security Frame Work for Smart IoT Environment using Received Signal Strength

Tawseef Naqishbandi[1], Zahid Gulzar Khaki[2]
[1]*Department of Computer Science and Engineering, IUST, Awantipora, J&K*
[2]*Department of Electronics and Communication, Engineering IUST, Awantipora J&K*

Abstract: ***The aim of this paper is to create a secret key between two different IoT wireless entities while not the necessity for sharing the key manually. The idea behind this is to generate the key based on the received signal strength (RSS) of the wireless signals. The RSS would be different for the two entities that are involved in communication based on their location and environment. Eavesdropper would not be able to detect these secret keys because the hacker would be located in a position other than the entities involved in the communication. This means that the RSS would be unique between any two entities and the signals and their strengths would not be the same for the hacker. Hence the secret bits abstracted out of the RSS which are falling outside the threshold levels will be definitely unique. This creates a novel plan & unique idea of creating the secret bits. The same calculation will be done on both the entities and eventually they will communicate with each other to come to a common shared key. Once the secret key is finalized, then the communication will begin with enhanced or increased security than before.***

Keywords: Internet of Things, Cryptography, Extraction, Signal, Received Signal Strength, Wireless. Key,

I. INTRODUCTION

The effectiveness of secret key extraction, for private communication between two smart sensible wireless nodes i.e. IoT devices [1], from the received signal strength (RSS) variations on the wireless channel between the two smart devices are being evaluated & studied. The real world measurements of RSS in a variety of environments and settings are used. While RSS is included in most commercial hardware platforms, researchers have expressed doubts about the reliability of RSS measurements [3,5,8,10],especially from beacons that are a considerable distance from the localizing node[2]. The study of 802.11 b/g network and using available APs in a real-time work environment, based laptops show that:

A. In certain smart environments i.e Internet Of Things (IOT) [1], due to lack of variations in the wireless channel, the extracted bits have very low entropy making these bits unsuitable for a secret key.
B. An adversary can cause predictable key generations in these static environments, and
C. In dynamic scenarios where the two smart devices are mobile, and/or where there is a significant moment in the environment, high entropy bits are obtained fairly quickly.

Building on the strengths of existing secret key extraction approaches, an environment adaptive secret key generation scheme that uses an adaptive lossyquantizer in conjunction with cascade-based information reconciliation and privacy amplification is being developed. The measurements show that the scheme, in comparison to the existing ones that are being evaluated, performs the best in terms of generation high entropy bits at a high bit rate. This secret key bit streams generated by the scheme also pass the randomness test in the NIST[5] test suite that are conducted. Its built and evaluated the performance of secret key extraction using small, low power, hand held devices-Google Nexus One phones-that are equipped 802.11 wireless network cards. Last, the secret key extraction in a multiple input multiple outputs (MIME)-like sensor network tested that is created using multiple Telos B sensor nodes was evaluated. It was found that the MIMO-like sensor environment produces prohibitively high bit mismatch, which is addressed using an iterative distillation stage that is added to the key extraction process. Ultimately, it was shown that the secret key generation rate is increased when multiple sensors are involved in the key extraction process. The effectiveness of secret key extraction, for private communication between two wireless devices, from the received signal strength (RSS) variations on the wireless channel between the two devices are being evaluated, studied and experimented. The real world measurements of RSS in a variety of environments and settings are used.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

II. PROBLEM DEFNITION

The security concerns while communicating between smart wireless devices have become a major research concern now-a-days. Since there is a huge exponential growth of smart wireless devices i.e Internet Of Things (IOT) in the world today, needless to say that the need for security has increased exponentially. The knowledge of the hackers has also been increased and they try to find every opportunity to attack the smart wireless device user or steal his/her data without his knowledge. To totally avoid the scenario and to provide a fool proof methodology of security the communication data is need of the hour today.

III. PROBLEM STATEMENT

Any communication between wireless devices if it has to be protected has to be encrypted and send across. For this encryption to happen, a secret key is needed. This secret key has to be shared between the two (or more) users who are going to communicate. This generation of the secret keys and sharing between the users will become a problem by itself let alone the security of the communication. The secret keys generated has to be communicated in a more fool proof way. The best way to share the secret key is just by whispering the key in the other party ears. It cannot be transferred through any other medium. But transferring the key by this way is not at all practical and hence there is a big problem in communicating this key which forms the basis for the further communication to happen.

IV. SYSTEM ANALYSIS

A. Existing System

Secret key establishment is a fundamental requirement for private communication between two IoT entities. Currently, the most common method for establishing a secret key is by using public key cryptography. However, public key cryptography consumes significant amount of computing resources problem of sharing secret keys between wireless nodes (say Alice and Bob) is to extract secret bits from the inherently random spatial and temporal variations of the reciprocal wireless channel between them. Essentially, the radio channel is a time and space-varying filter, that at any point in time has the identical filter response for signals sent from Alice to Bob as for signals sent from Bob to Alice.

B. Limitations of Existing System

Significant amount of computing resources and power are required to achieve the public key cryptography which might not be available in certain scenarios like sensor networks[2]. Using other forms of cryptography which do not use public key methods are Quantum Cryptography which are still very rare and expensive.

V. PROPOSED SYSTEM

Received signal strength (RSS) is a popular statistic of the radio channel and can be used as the source of secret information shared between a transmitter and receiver. We use RSS as a channel statistic, primarily because of the fact that most of the current of-the-shelf wireless cards, without any modification, can measure it on a per frame basis. The variation over time of the RSS, which is caused by motion and multipath fading, can be quantized and used for generating secret keys. The mean RSS value, a somewhat predictable function of distance, must be filtered out of the measured RSS signal to ensure that an attacker cannot use the knowledge of the distance between key establishing entities to guess some portions of the key. These RSS temporal variations, as measured by Alice and Bob, cannot be measured by an eavesdropper (say Eve) from another location unless she is physically very close to Alice or Bob. However, due to non-ideal conditions, including limited capabilities of the wireless hardware, Alice and Bob are unable to obtain identical measurements of the channel. This asymmetry in measurements brings up the challenge of how to make Alice and Bob agree upon the same bits without giving out too much information on the channel that can be used by Eve to recreate bits between Alice and Bob.

A. Advantages of proposed system

1) It's very cost effective, since the current wireless adapters that are current prevailing in the market have the capability to calculate the RSS measurements of the signal strength and converting them into dBm values[12].

2) The secret key produced is very much dependent on the environment and distance between the two parties involved in the communication. Hence it makes practically impossible for an eavesdropper to guess the key generation or to act as a middle man in the communication. The key idea behind this is to extract secret keys by both the parties independently without

communicating with each other. The extract the key based on the receiver signal strength between the entities and hence there is no way a third person will be able to guess the key or portions of it.

VI. PROPOSED SYSTEM FRAMEWORK

Extraction of received signal strengths , as multiple packets are exchanged between Entity-1 and Entity-2 (Fig.1), each of them builds a time series of measured RSS. Then, each node quantizes its time series to generate an initial secret bit sequence. The quantization is done based on specified on thresholds. The received signal strength is calculated for received signals and is plotted in a graph to pic the bits which lie outside the psitive and negative threshold levels.

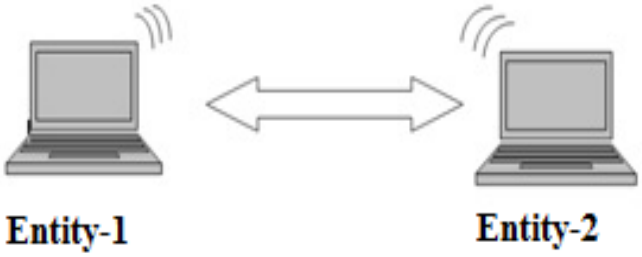


Fig.1. Flow Depicting Exchange of Packets

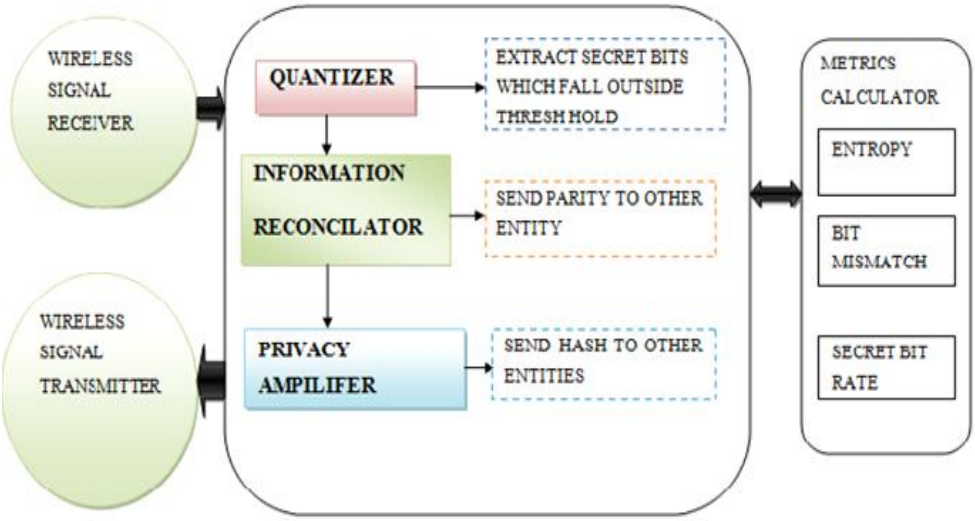


Fig.2. System Frame work Design

The system frame work design is depicted in Fig.2.The main entities involed are wirless receiver and transmitter. Fig 2. Can be further broadly understood bv dividing it further as shown in Fig.3.depicted below. Wirless Signal Receiver signal output goes to the quantizer then to quantizers output goes as input to information Reconcilator

Fig.3. Level 0 Data flow Diagram

The Information Reconcilator the passes its output to privacy amplifier and finally the output from privacy amplifier reaches to the wireless signal transmitter. The other main module description is further discussed as under:-

A. Parity Bit Generation

Once both Entity-1 and Entity-2 as depicted in Fig.1.extract the bit stream from the RSS measurements they collect using quantizers, to agree upon the same key, they must correct the bits where the two bits streams differ. Cascade is an iterative, interactive information reconciliation protocol. In this protocol, Entity-1 permutes the bit stream randomly, divides it into small blocks, and sends permutation and parity information of each block to Entity-2.

Entity-2 permutes his bitstream in the same way, divides it into same blocks, computes parities and checks for parity mismatches. For each mismatch, Entity-2 performs a binary search on the block to find if a few bits can be changed to make the block match the parity. These steps are iterated a number of times to ensure a high probability of success. The Further level and data flow of Fig 2. Can be illustrated in Fig.4 for better understanding as depicted below

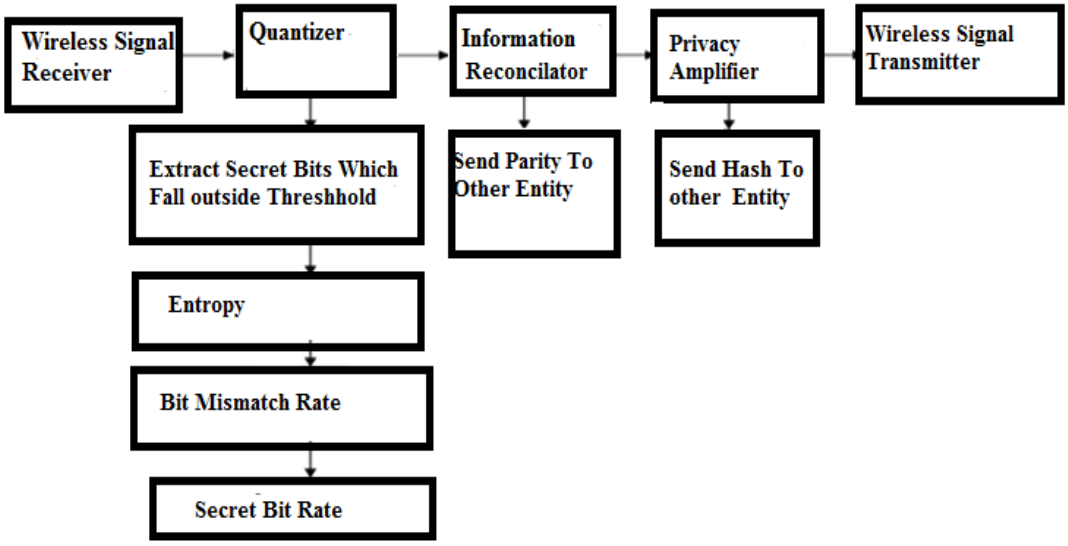


Fig.4 Level 1 Data flow Diagram

B. Privacy Amplification

Privacy Amplification generates a shorter secret bit stream with a higher entropy rate from a longer secret bit stream with a lower entropy rate. Privacy Amplification are based on the leftover hash lemma, a well-known technique to extract randomness from imperfect random sources.

C. Metrics Calculation

Entropy characterizes the uncertainty associated with a random variable. We estimate the entropy of a bit stream using NIST [5] test suite's approximate entropy test. We define the bit mismatch rate as the ratio of the number of bits that do not match between Entity-1 and Entity-2 to the number of bits extracted from RSS quantization. We define secret bit rate as the average number of secret bits extracted per collected measurement. This rate is measured in terms of final output bits produced after taking care of bit losses due to information reconciliation and privacy amplification.

D. Adaptive Secret Bit Generation

Entity-1 and Entity-2 consider a block of consecutive measurements of size block size which is a configurable parameter. 1 for each block, they calculate two adaptive thresholds q+ and q- independently such that q+ = mean + α* std deviation and q- = mean –α* std deviation, where $\alpha > 0$. Entity-1 and Entity-2 parse their RSS measurements and drop RSS estimates that lie between q+ and q- and maintain a list of indices to track the RSS estimates that are dropped. They exchange their lists of dropped RSS estimates and only keep the once that they both decide not to drop. Entity-1 and Entity-2 generate their bit streams by extracting a 1 or a 0 for each RSS estimate if the estimate lies above q+ or below q-, respectively.

VII. CONCLUSION

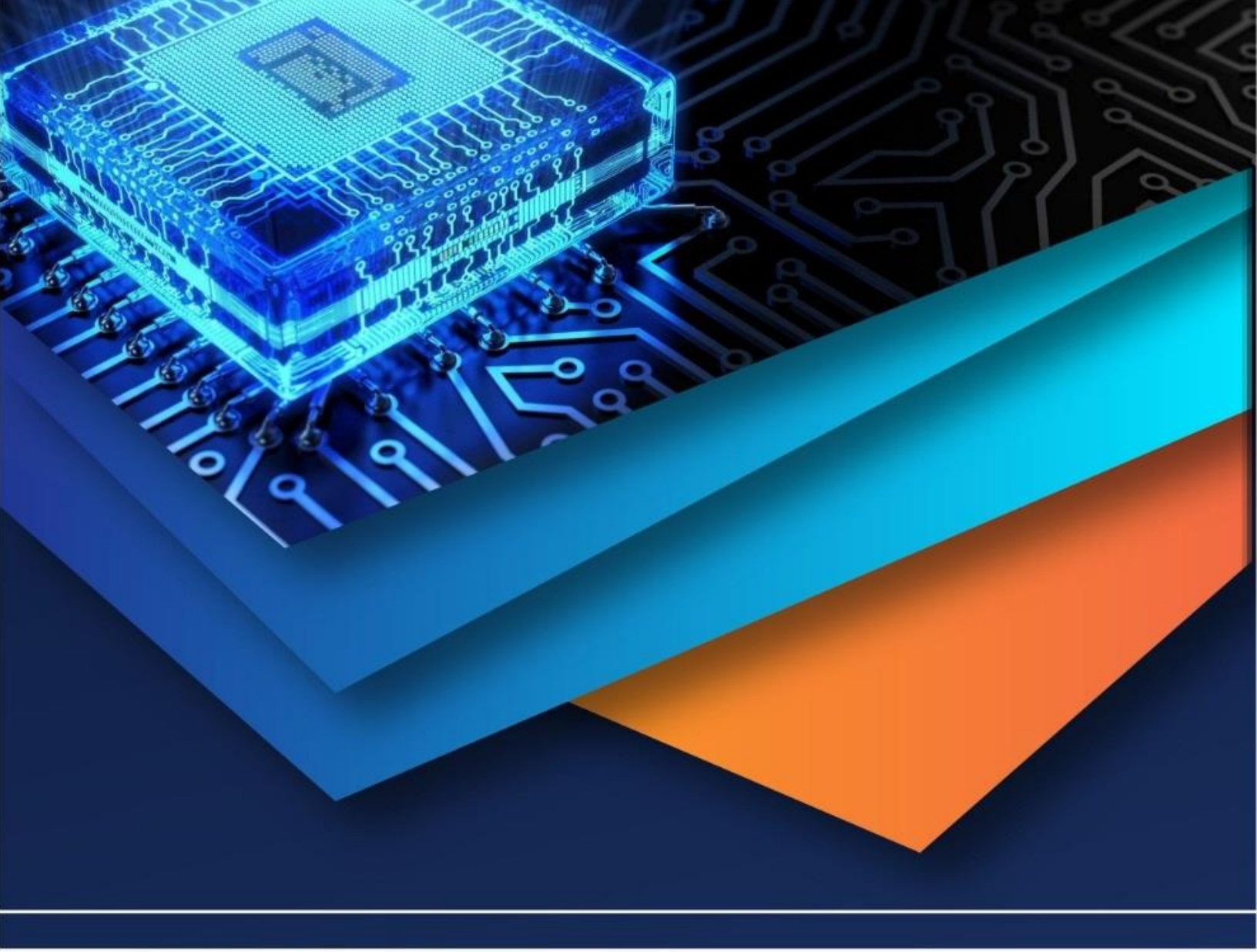
The effectiveness of secret key extraction from the RSS variations in wireless channels using extensive real world measurements in a variety of environments and setting is evaluated. The frame work analysis approach suggest that bits extracted in static environments are unsuitable for generating a secret key. It was found that adversary can cause predictable key generation in static environments.. The aim of this paper in future is to develop an environment adaptive secret key generation scheme for generating high entropy bits at a high bit rate in comparison to the existing ones that are evaluated.

VIII. ACKNOWLEDGEMENT

The authors acknowledge valuable contribution from anonymous reviewers, and useful discussion with Er. Syed Mujtiba, Assistant Professor Department of Computer Science and Engineering, IUST, Awantipora, J&K

REFERENCES

[1] Tawseef Ahmad Naqishbandi and Imthyaz Sheriff, C.: Big Data, CEP and IoT : Redefining Healthcare Information Systems and Analytics. International Conference on Advances Research in Engineering and Technology (2014)
[2] C. Komar, and C. Ersoy, "Location Tracking and Location Based Service Using IEEE 802.11 WLAN Infrastructure," in Proc. of the European Wireless Workshop, February 2004
[3] Weng Kai and Chen Chun; "Using RSS with difference method in localization algorithm for sensor networks", 2nd International Conference on Information Science and Engineering (ICISE), 2010; pp. 2500 – 2502
[4] N. Bulusu, J. Heidemann, and D. Estrin. GPS-less low-cost outdoor localization for very small devices. IEEE Personal Communications, 7(5):28–34, October 2000.
[5] NIST, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf,2001
[6] and J.-P. Hubaux. Secure positioning of wireless device ˇ s with application to sensor networks. In Proc. 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05), Miami, FL, USA, March 2005.
[7] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher. Rangefree localization schemes for large scale sensor networks. In Proc. 9th Annual International Conference on Mobile Computing and Networking, (MobiCom'03), pages 81–95, San Diego, CA, USA, 2003.
[8] Y. M. Kwon, K. Mechitov, S. Sundresh, W. Kim, and G. Agha. Resilient localization for sensor networks in outdoor environments. In Proc. 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), pages 643–652, Columbus, OH, USA, June 200
[9] B.Azmi-sadjadi, A. Kiayas, A. Mercado, and B. Yener, "Robust Key Generation from signal enevolops in Wireless Networks," proc.14th ACM Conf. Computer and Comm. Security (CCS), 2007.
[10] C.H.Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental Quantum Cryptography" J.Cryptology, vol.5, no. 1, pp.3-28, 1992.
[11] S.Mathur, W.Trappe, N.B.Mandayam, C.Ye, and A.Reznik, "Radio-Telepathy: Extracting a secret key from an Unauthenticated Wireless Channel," Proc. ACM MobiCom,2008.
[12] Converting signal strength percentage to dBm values," http://www.wildpackets.com/elements/whitepapers/converting_signal_strength.pdf,2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY