

# A Secured Approach for Secret Key Extraction from Wireless Signal Strength Preserving Authentication and Security

Mary Leema Rose. A

Computer Science and Engineering

Prathyusha Institute of Technology and Management, India.

## Abstract—

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 and power which might not be available in certain scenarios. Hence this project discovers the scheme which implements the concept, when source sends a data to the destination, data is being forwarded to the intermediate nodes one by one, based on Received Signal Strength (RSS) secret key will be generated which is passed to both the source and the destination. A random key will be parsed by both source and destination which is exchanged between both for verification. Both of them generates hash key value of the secret keys, which will also be verified by both of them only then the data can be viewed by the destination. Thus a strong verification scheme at the destination end can be achieved. This ensures authentication of the source and destination. Authentication is a primitive that enables a node to ensure the identity of peer node with which it is communicating with. Hence the security level will be increased by using the Secret Key Extraction mechanism.

**Keywords—** Authentication, Security, RSS, Handler node, RC4 Encryption, Node Frame Initiation.

## I. INTRODUCTION

In today's computing world, different technologies have come up. These have grown to support existing computer networks all over the world. With mobile computing, one can find that the need to be confined within one physical location has been eradicated. Hearing of terms such as telecommuting enables anyone to work from home or the field but at the same time accessing resources as if one is in the office. The emergence of portable computers and laptops, personal digital Assistants (PDA), PC Tablets and Smart phones, has in turn made mobile computing very convenient. The portability of the devices ensures and enables user to access all services as if they were in the internal network of their company. For example, the use of Tablet PC and Ipads. This new technology enables users to update documents, surf the internet, send and receive e-mail, stream live video files, take photographs and also support video and voice conferencing.

Secret key establishment is a fundamental requirement for private communication between two entities. Currently, the most common method for establishing a secret key is by using public key cryptography. Most of the previous research work on RSS-based secret key extraction, including that is based on either simulations or theoretical analysis. Other than the recent work that was performed in a specific indoor environment, there is very little research on evaluating how effective RSS-based key extraction is in real environments under real settings. Proposed scheme address this important limitation of the existing research in this paper with the help of wide-scale real life measurements in both static and dynamic environments.

## II. EXISTING SYSTEM & ITS DISADVANTAGES

A less expensive solution that uses inherent randomness in wireless channel to extract secret key bits based on the RSS (Received Signal Strength) was developed in the existing one. Environment adaptive secret key generation scheme using quantization, information reconciliation and privacy amplification was developed. RSS measurements were determined by periodically exchanging the probe packets and finding the Range (*max and min*) and performing the three above process. Thus the secret key was extracted from the received signal strength variations on wireless channel. The principle involved is, Once Alice and Bob collect the RSS measurements they perform the following steps:

1. Determine the Range of RSS measurements from the minimum and the maximum measured RSS values
2. Find N, the number of bits that can be extracted per measurement, where  $N \leq \log_2 \text{Range}$
3. Divide the Range into  $M = 2^n$  equal sized intervals
4. Choose an N bit assignment for each of the M intervals
5. For each RSS measurement, extract N bits depending on the interval in which the RSS measurement lies.

After completing the above steps, as in the single bit extraction case, Alice and Bob use information reconciliation to correct the mismatching bits, and finally, apply privacy amplification to the reconciled bit stream and extract a high entropy bit stream. Thus the results show that our single bit extraction in conjunction with information reconciliation and privacy amplification is able to achieve higher entropy in comparison to existing schemes, and our multiple bit enhancements allows to significantly increase the secret bit rate as well.

Various disadvantages have been found while two wireless devices are participating in a private communication [10], with reference to other surveyed papers some of the major drawbacks are listed below:

- Security is very low in the existing system. Generally security is considered to be the most important and crucial factor that need to be present in all the system. But in the existing system, this becomes a lacking factor.
- The verification of authenticated source and destination is not available in the existing system. Authentication often involves verifying the validity of at least one form of identification that mainly lacks in the existing system.
- In the existing system, specifically there are more possibilities of predictable channel attacks. One such example is side channel attack. Thus it leads to very low security.
- Hackers can easily hack the data or interrupt the communication.

### III. PROPOSED SYSTEM & ITS OBJECTIVE

The main objective is to develop a strong verification scheme at the destination end. To design and implement the authentication of the source and destination by defining a key extraction algorithm and a framework for wireless devices for secure data transmission.

The proposed system mainly concentrates in solving the disadvantages experienced in the existing one[10], hence the proposed scheme revolves around the concept, when source sends a data to the destination, data is being forwarded to the intermediate nodes one by one, based on Received Signal Strength (RSS) secret key will be generated which is passed to both the source and the destination. A random key is being parsed by both source and destination which is exchanged between each other for verification. This random key is generated from the secret key bits and both the source and destination exchanges and verifies simultaneously. Both of them then generate hash key value of the secret keys which is also verified by both of them. After the secret key, random key, hash key value and the decryption key is verified only then the data can be viewed by the destination. Network is constructed with the sign in option so that each node can be assigned with the time frames that showcase the mobility nature of the node. Thus the node frame initialization plays a vital role in the system construction followed by the login of the node that makes the node active inside the network. After the login in the node will encrypt the data using RC4 and sends the data to the destination which contains all the following verification to be done then the data can be viewed by the destination.

Advantages that mark the unique nature of the proposed system are listed as follows. These advantages make the systems security get enhanced to a greater level.

- The verification of authenticated source and destination will be achieved in the proposed system since this involves secret key verification along with random key, hash key value and the decryption key.
- Authentication often involves verifying the validity of at least one form of identification that mainly lacks in the existing system. The genuinely source can be identified by this manner.
- The proposed system will provide a strong verification scheme at the destination end.
- Thus the security level will be increased and enhanced from the existing level of security by using this secured approach of Secret Key Extraction Mechanism.

### IV. SYSTEM ARCHITECTURE

The system architecture mainly describes the system being divided into six major modules namely, node frame initiation, handler node, encryption mechanism, key generation based on RSS, random number generation and key authentication. The system architecture depicts how the data is being forwarded after the network construction. The network initiation involves the node frame initialization that assigns time frame to each node. Implementation specifically involves the network construction in which the node frame initialization plays a vital role. In node frame initialization, each node that logs in into the system is assigned with the time frame that depicts the mobile nature of the node. Handler node focus on all the monitoring activity of the nodes that are active in the network and also update the necessary details in the database concerned. Encryption is based on the RC4 algorithm and the particular node selects the file to be encrypted, enters the key and encrypts it and sends to the destination. After the file is encrypted the source

sends the encrypted data to the destination, then secret key is generated based on RSS and from the secret key random key is generated. Hash value of the key along with all these combinations are used to make the transmission secured and authenticated.

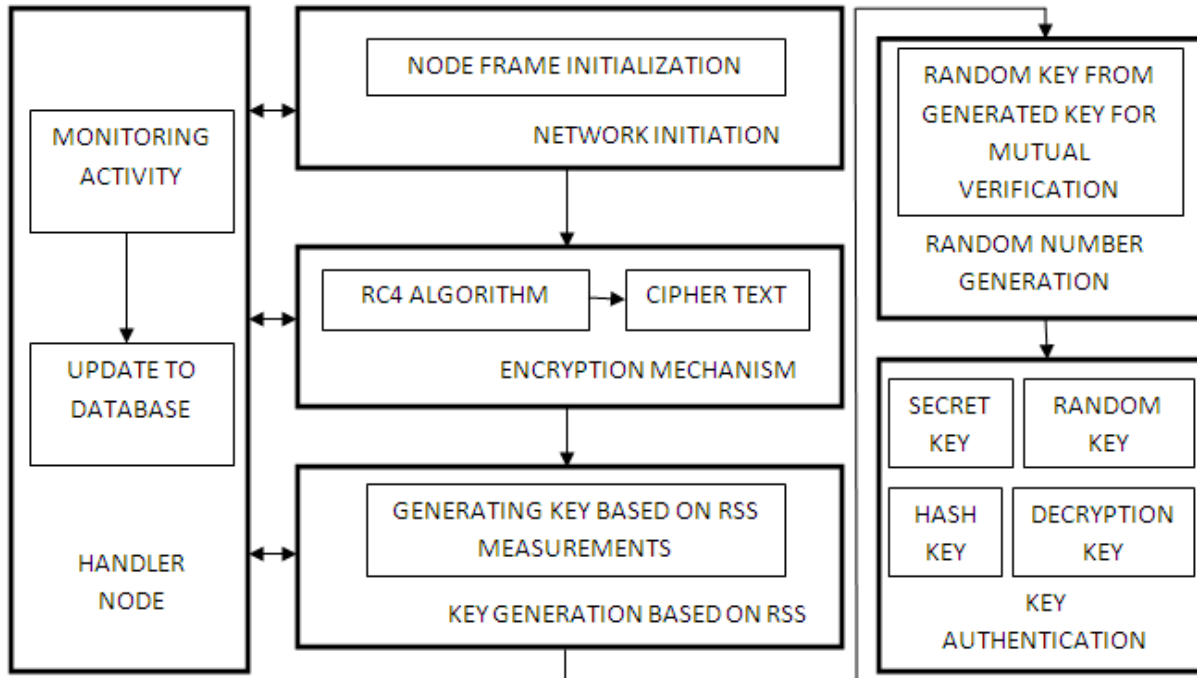


Fig. 1 Architecture diagram

## V. SURVEY RESULTS

The literature survey is mainly carried out by analysing a series of papers which highlights especially how RSS has been used for efficient secret key generation, and how other factors proposed can make the system get enhanced in security level. Secret key is extracted from the Received Signal Strength (RSS) but security level is very low. Thus the author's of [21] addresses that security and authentication is not considered in the paper. Hence the proposed scheme highlights to include the authentication to the existing one. From the experimental results shown in [7] the proposed scheme has the ability to generate Secret keys from the RSSI profile with sufficient independence. This is the possible solution that will allow the system to use ESPAR antennas that focus on extracting secret bits with high entropy rate. The conclusion drawn from the paper [10] depicts the importance of concentration on the security of the wireless link. It focuses on the message confidentiality, integrity and mainly authentication. Thus robust key with authentication can be created even if interference exists. The results from series of experiments [11] observation related to the proposed scheme shows that in secret key sharing mechanism, encryption of information also results in secured way of communication. Observation from the paper [13] depicts that efficiency is got from hash value over the value indications and random key can be used to achieve secrecy authentication. Basic idea that revolves in the paper [16] depicts that even in the varying channel state, stable secret key bits can be generated and high level security can be achieved. Observation related to the new scheme [17] is that it is possible to convert from one unit to another, albeit with varying degrees of accuracy, RSSI is more effective and easy way of measurement of signal strength. From [19] the practical features of PRNGs such as high generation speed, good statistical properties and no need for additional hardware devices made these generators very attractive and are the most widely used RNGs. Thus pseudo random number generator is more effective.

## VI. CONCLUSIONS

The effectiveness of secret key extraction from the RSS variations in wireless channels using extensive real world measurements in a variety of environments and settings is considered. Proposed system addresses the scheme in which, when source sends a data to the destination, data is being forwarded to the intermediate nodes one by one, based on Received Signal Strength (RSS) secret key will be generated which is passed to both the source and the destination. Main concentration prevails on the first three modules namely node frame initiation, handler node and encryption mechanism. Implementation specifically involves the network construction in which the node frame initialization plays a vital role. In node frame initialization, each node that logs in to the system is assigned with the time frame that depicts the mobile nature of the node. Handler node focus on all the monitoring activity of the nodes that are active in the

network and also update the necessary details in the database concerned. Encryption is based on the RC4 algorithm and the particular node selects the file to be encrypted, enters the key and encrypts it and sends to the destination. The conclusions drawn in this project, specifically details the predictable channel attack, that are primarily for key extraction using RSS measurements can be resolved by unpredictable encryption technique. Future work of this project addresses how authentication will be implemented and the time complexity will be reduced. This project would like to explore this in mere future.

#### REFERENCES

- [1] S. Wiesner, "Conjugate Coding," SIGACT News, vol. 15, no. 1, pp. 78-88, 1983.
- [2] U.M. Maurer, "Secret Key Agreement by Public Discussion from Common Information," IEEE Trans. Information Theory, vol. 39, no. 3, pp. 733-742, May 1993.
- [3] G. Brassard and L. Salvail, "Secret Key Reconciliation by Public Discussion," Proc. Workshop Theory and Application of Cryptographic Techniques on Advances in Cryptology, pp. 410-423, 1994.
- [4] J.E. Hershey, A.A. Hassan, and R. Yarlagadda, "Unconventional Cryptographic Keying Variable Management," IEEE Trans. Comm., vol. 43, no. 1, pp. 3-6, Jan. 1995.
- [5] M.A. Tope and J.C. McEachen, "Unconditionally Secure Communications over Fading Channels," Proc. IEEE Military Comm. Conf. (MILCOM), 2001.
- [6] G.D. Durgin, Space-Time Wireless Channels. Prentice Hall PTR, 2002.
- [7] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels," IEEE Trans. Antennas and Propagation, vol. 53, no. 11, pp. 3776-3784, Nov. 2005.
- [8] C. Ye, A. Reznik, and Y. Shah, "Extracting Secrecy from Jointly Gaussian Random Variables," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2006.
- [9] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing Wireless Systems via Lower Layer Enforcements," Proc. Fifth ACM Workshop Wireless Security (WiSe), 2006.
- [10] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust Key Generation from Signal Envelopes in Wireless Networks," Proc. 14th ACM Conf. Computer and Comm. Security (CCS), 2007.
- [11] Robert Wilson, David Tse, and Robert A. Scholtz, "Channel Identification: Secret Sharing Using Reciprocity in Ultra wideband Channels", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol. 2, No. 3, September 2007.
- [12] L. Greenemeier, "Election Fix? Switzerland Tests Quantum Cryptography," Scientific Am., Oct. 2007.
- [13] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin, "Wireless Information-Theoretic Security," IEEE Trans. Information Theory, vol. 54, no. 6, pp. 2515-2534, June 2008.
- [14] A. Sayeed and A. Perrig, "Secure Wireless Communications: Secret Keys through Multipath," Proc. IEEE Int'l Conf. Acoustics, Speech Signal Processing (ICASSP), pp. 3013-3016, Apr. 2008.
- [15] S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N. Patwari, and S.V. Krishnamurthy, "On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments," Proc. ACM MobiCom, 2009.
- [16] Chunxuan Ye, Suhas Mathur, Alex Reznik, Yogendra Shah, Wade Trappe, and Narayan B. Mandayam "Information-Theoretically Secret Key Generation for Fading Wireless Channels", IEEE Transaction on INFORMATION FORENSICS AND SECURITY, vol. 5, no. 2, June 2010.
- [17] "Converting Signal Strength Percentage to dBm Values," [http://www.wildpackets.com/elements/whitepapers/Converting\\_Signal\\_Strength.pdf](http://www.wildpackets.com/elements/whitepapers/Converting_Signal_Strength.pdf), 2012.
- [18] "ipwraw," [http://homepages.tu-darmstadt.de/~p\\_larbig/wlan](http://homepages.tu-darmstadt.de/~p_larbig/wlan), 2012.
- [19] Kinga MÁRTON , Alin SUCIU , Christian SĂCĂREA , Octavian CREȚ "Generation and Testing of Random Numbers cryptographic Applications" ,PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A, Volume 13, Number 4/2012, pp. 368-377.
- [20] "Radiotap," <http://www.radiotap.org>, 2012.
- [21] Sriram Nandha Premnath, Suman Jana, Jessica Croft, Prarthana Lakshmane Gowda, Mike Clark, Sneha Kumar Kasera, Neal Patwari, and Srikanth V. Krishnamurthy, *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 12, no. 5, pp.917-930, MAY 2013.