© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Secrete Key Extraction Using Received Signal Strength (RSS) of Wireless Networks

Solai Rajan T, Udaya Kumar D J, Anima Mahato
Information Technology, Dhanalakshmi College of Engineering, Chennai, Tamil Nadu, India

ABSTRACT

In this paper, we evaluate the effectiveness of secret key extraction from the Received signal strength (RSS) variations on the wireless channel between the two devices for private communication between them. We use real world measurements of RSS in a variety of environments and settings. The results from our experiments with 802.11-based laptops show that 1)An adversary can cause predictable key generation in these static environments, and 2)In dynamic scenarios where the two devices are mobile, high entropy bits are obtained . Building on the strengths of existing secret key extraction approaches, we develop an environment adaptive secret key generation scheme that uses an adaptive Cascade-based information reconciliation and privacy amplification. In our scheme, to provide good scalability in terms of the number of nodes, we utilize a combinatorial design of public-private key pairs, which means nodes combine more than one key pair to encrypt and decrypt messages. We also show that it provides controllable resilience when malicious nodes compromise a limited number of nodes before key revocation and renewal.

Keywords: Secrete Key Extraction, Key generation, Key exchange

I. INTRODUCTION

Secret Key establishment is a basic requirement for private communication between two entities. We use a 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 (e.g., sensor networks). More importantly, concerns about the security of public keys in the future have spawned research on methods that do not use public keys.

II. METHODS AND MATERIAL

Related Works

A. Wireless Information-Theoretic Security

This paper considers the transmission of confidential data over wireless channels. Based on an information-theoretic formulation of the problem, in which two legitimates partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent quasi-static fading channel, the important role of fading is characterized in terms of average secure communication rates and outage probability. Based on the insights from this analysis, a practical secure communication protocol is developed, which uses a four-step procedure to ensure wireless information-theoretic security: (i) common randomness via opportunistic transmission, (ii) message reconciliation, (iii) common key generation via privacy amplification, and (iv) message protection with a secret key. A reconciliation procedure based on multilevel coding and optimized low-density parity-check (LDPC) codes is introduced, which allows to achieve communication rates close to the fundamental security limits in several relevant instances. Finally, a set of metrics for assessing average secure key generation rates is established, and it is shown that

the protocol is effective in secure key renewal-even in the presence of imperfect channel state information.

B. Unconditionally Secure Communication over Fading Channels

In this paper, we propose a novel method for two communicates to exchange a secret over a public wireless fading channel. Unlike conventional computationally secure public key methods, this technique is information theoretic and unconditionally secure provided that a component of the reciprocal channel fading over time between the two communicates is statistically independent with the channel fading from either communicate to the eavesdropper. This technique may be particularly well suited to secure tactical mobile communications. A simple protocol suitable for a lognormal shadowed fading channel is described and its key exchange rate is derived

C. Secure Wireless Communication:

Secret Keys through Multipath Secure wireless communications is a challenging problem due to the shared nature of the wireless medium. Most existing security protocols apply cryptographic techniques for bit scrambling at the application layer by exploiting a shared secret key between pairs of communicating nodes. However, more recent research argues that multipath propagation – a salient feature of wireless channels – provides a physical resource for secure communications. In this context, we propose a protocol that exploits the inherent randomness in multipath wireless channels for generating secret keys through channel estimation and quantization. Our approach is particularly attractive in wideband channels which exhibit a large number of statistically independent degrees of freedom (DoF), thereby enabling the generation of large, more-secure, keys. We show that the resulting keys are distinct for distinct pairwise links with a probability that increases exponentially with the key-size/channel DoF. We also characterize the probability that the two users sharing a common link generate the same key. This characterization is used to analyze the energy consumption in successful acquisition of a secret key by the two users. For a given key size, our results show that there is an optimum transmits power, and an optimum quantization strategy, that minimizes the energy consumption. The proposed approach to secret key generation through channel quantization also obviates the problem of key pre- distribution inherent to many existing cryptographic approaches.

PROPOSED SYSTEM MODEL

In this proposed model, the advances in cost-effective sensing, computing, and communication wireless devices. The proposed systems are composed of mobile, autonomous, wireless devices and Secret key extraction, for secure communication between two wireless devices, from the Received signal strength (RSS) variations on the wireless channel between the two devices. It Fulfil the required attributes of secure communications, such as data integrity, authentication, confidentiality, non-repudiation and service availability. The design of public key management schemes that would

Step1: Encryption: If the Source nodes want to the Send the data to the destination node, they will choose the destination Id. Then they have to choose the file from its directory. Once chosen the Data, it will be Encrypted using RC4 algorithm. Once encrypted the data will send to the Destination node via intermediate nodes. We may able to see the path of the data traveling in the Source/ Destination Nodes frame.

Step2: Key Generation Based on RSS: Once the Data is Encrypted, the data will send to the chosen Destination node via the intermediate nodes in the network. While the is transmitted using via intermediate node, they will generate a Key using Key Extraction Algorithm based on Received Signal Strength. These key will be Share to the Source and Destination nodes by the intermediate nodes till the data packets reaches the Destination Node.

Step 3: Random Number Generation: Once the data reaches the destination node mutual verification is

attained in the both Source and Destination nodes by sharing the key generated by the intermediate nodes. To implement this concept, we can generate a Random number from the keys shared by the intermediate and verify the key was presented in the Destination Node. If present then other authentication process will be held. If not then the destination node will not able to the receive data.

Step 4: Primary Key and Master Key and Authentication: Once the Mutual Verification process is finished, the destination node's information like User Name, Password and IP address along with the Primary Key and Master Key. This information will be verified for authentication Process. Also the Hash values are also verified. Once this information is verified, the Destination node wants to provide the decryption key to decrypt the Original data. All these condition are satisfied and then only the destination node is allowed to access the original data.

SYSTEM ARCHITECTURE

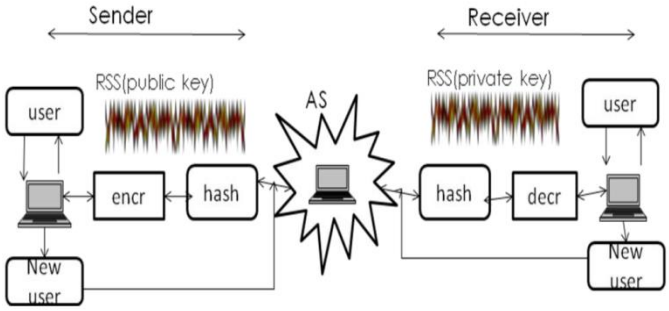

Figure 1: Proposed System Architecture

The above architecture tells about the required attributes of secure communications, such as data integrity, authentication, confidentiality, non-repudiation and service availability.

III. RESULTS AND DISCUSSION

The proposed framework is implemented and tested on simulation of simple cloud setup with the help of .NET framework 3.5 The plain text is encrypted by Triple DES algorithm and the Public key is generated from the Received Signal Strength (RSS).

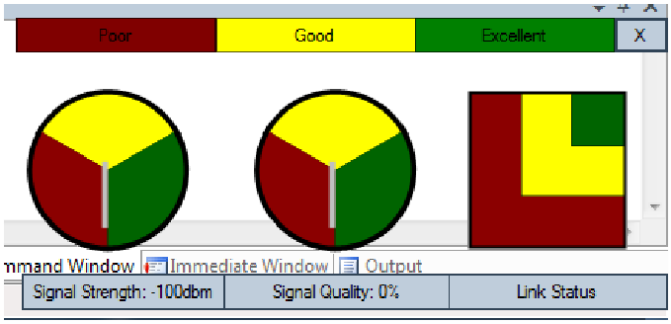

Figure 2: Wireless Signal Indicator

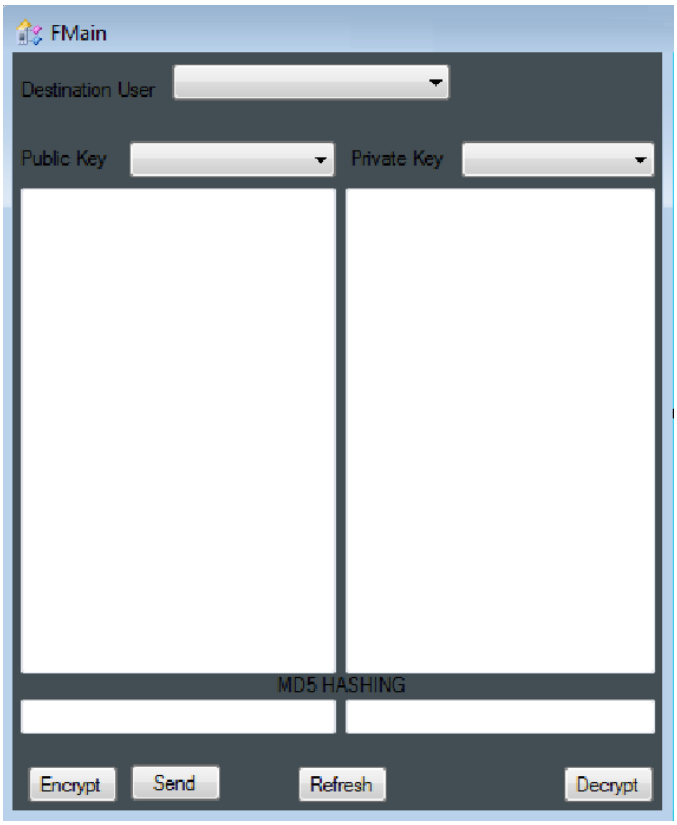

Figure 3: Encryption and Key Generation

IV. CONCLUSION

In this paper, we evaluated 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. Our experimental results showed that bits extracted in static environments are unsuitable for generating a secret key. We also found that an adversary can cause predictable key generation in static environments. However, bits extracted in dynamic environments showed a much higher secret bit rate. We developed an environment adaptive secret key generation scheme and our measurements showed that our scheme performed the best in terms of

generating high entropy bits at a high bit rate in comparison to the existing ones that we evaluated. The secret key bit streams generated by our scheme also passed the randomness tests of the NIST test suite that we conducted. We were able to further enhance the rate of secret bit generation of our scheme by extracting multiple bits from each RSS measurement. We also evaluated secret key extraction in a MIMO-like sensor network tested and showed that secret key generation rate can be improved by involving multiple sensors in the key extraction process. The conclusions drawn in this paper, specifically the predictable channel attack, are primarily for key extraction using RSS measurements, and these may not directly apply to key extraction using channel impulse response measurements. We would like to explore this in our future work.

V. REFERENCES

[1] W. Stallings "Cryptography and network security principles and practice," Fourth edition, Prentice hall, 2007.

[2] Gope, P., Ghosh, D., Chelluri, A.R.K. and Chattopadhyay,P., 2009. Multi Operator Delimiter based Data Encryption Standard (MODDES). ICCNT. Chennai, India, June 27 – 29. 2009.

[3] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On technical security issues in cloud computing" 2009, IEEE Computer Society.

[4] M.Kallahalla, E.Riedel, R.Swaminathan, Q.Wang, and K.Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.Second USENIX Conf. File and Storage Technologies (FAST), pp.29-42,2003.

[5] C. Wang, Q.Wang, K.Ren, and W.Lou, "Privacy- Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE 29th Int'l Conf. Computer Comm. (INFOCOM), pp.525-533, 2010.

[6] C. Dubnicki, L.Gryz, L.Heldt, M.Kaczmarczyk, W.Kilian,P.Strzelczak,J.Szczepkowski,C.Ungurean, and M.Welnicki, "Hydrastor: A Scalable Secondary Storage," Proc. Seventh Conf. File and Storage Technologies (FAST), pp.197-210,2009.

[7] P.Druscheland A.Rowstron, "PAST: A Large- Scale, Persistent Peer-to-Peer Storage Utility," Proc. Eighth Workshop Hot Topics in Operating System (Hot OS VIII), pp.75-80,2001.

[8] G.Ateniese, K.Benson, and S.Hohenberger, "Key-Private Proxy Re-Encryption," Proc. Topics in Cryptology (CT-RSA), pp.279-294,2009.