SECURED KEY EXCHANGE BY INFORMATION RECONCILIATION AND PRIVACY AMPLIFICATION USING RECEIVED SIGNAL STRENGTH

P.Dharshini[1], S.Jayapriya[2], C.Sowmiya[3], Jesu Jayarin[4], Visumathi[5]

[1]*FinalYear B.E, CSE, Jeppiaar Engineering College, Tamilnadu, India*
[2]*FinalYear B.E, CSE, Jeppiaar Engineering College, Tamilnadu, India*
[3]*FinalYear B.E, CSE, Jeppiaar Engineering College, Tamilnadu, India*
[4]*Professor, CSE, Jeppiaar Engineering College, Tamilnadu, India*
[5]*Professor, CSE, Jeppiaar Engineering College, Tamilnadu, India*

Abstract

In order to make the communication more secure in the dynamic environment, the signal strength is used through which high entropy bit can be achieved. The received signal strength is used to find the nearest node in order to forward the data towards the destination node. In the existing system the secret key is generated only by the source and the destination nodes. In our proposed system, the secret key is generated by each and every hop. The generated key is quantized by the technique called quantization and the bit mismatch is reduced by information reconciliation technique. The bits that are lost during information reconciliation is avoided by distillation. In order to reduce the resultant output bit stream, hash key of the secret key is generated by using Privacy amplification technique. The low output bit stream result in high entropy. Here the predictable key generation is highly reduced. In this we are generating the random number to ensure data integrity and authentication. For this MNF hash function is used which is of 256 bits Privacy amplification is used to ensure that the resultant bit pattern is random. The mismatched bits can also be identified easily. Multiple sensors are involved in increasing the rate of the secret key generation. Generated bit streams are verified by randomness test. Our experiment has been implemented in 802.11A laptops.

***Keywords:** Received Signal Strength, Quantization, Information Reconciliation, Privacy Amplification, Hash key, Secret key.*

--***--

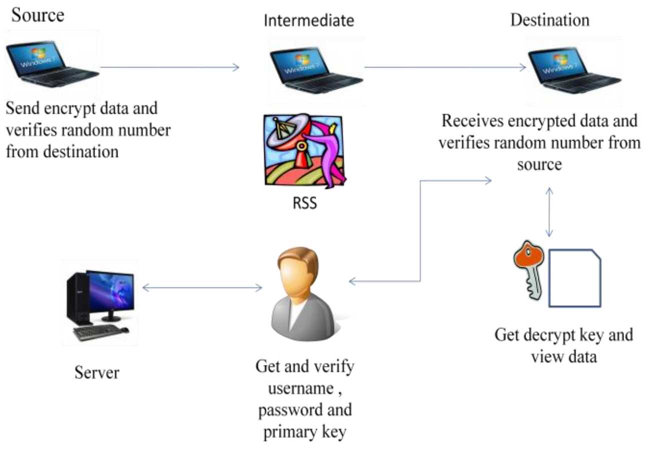
1. INTRODUCTION

Currently, Public Key Cryptography is used. But due to high power consumptions we are using Quantum Cryptography which is used for sharing a secret between nodes. Generating SECRET KEY is the basis for secured communication in dynamic environment. Quantum cryptography is still rare and costly. By receiving the signal strength , the secured message is transferred from sender to receiver. Signal strength is measured on a per frame basis, the result is quantized and it is used for key generation. Information reconciliation and privacy amplification supports RSS quantization techniques. The distance function that can be easily forecasted is removed while measuring the signal strength. Privacy amplification decreases the information rate that the attacker can have. More security is provided by the generation of secret key by every node, the random key and the hash key of the secret key. Time series is quantized to generate the secret key. In this paper we used the MNF hash function that takes a message of any length and promotes it to a hash value of 256 bits. The compression function has three parallel branches, each has sixteen words of 32 bits to eight words of 32 bits. In our project multiple bits is extracted in the place of single bit extraction.

2. EXISTING APPROACHES

Now, the general method for establishing a secret key is by using public key cryptography. But, this technique consumes significant amount of computing resources and power which is impossible in certain scenarios. More importantly, concerns about the security of public keys in the future have proved that the methods will never use public keys. The drawback in this is the security is very low and the hackers can easily hack the data or can easily interrupt the communication. In the existing system, during signal strength measurement more bits are dropped to maintain high entropy bit. So, our aim is to produce high entropy bit so that the resultant bit stream can be used directly as a shared secret key. In the most existing hardware, Amplitude can be measured easily than the time delay and it can be applied directly to common wireless networks here we use the same measurement of amplitude. To generate a secret between two nodes and to test the data that can be received by an eavesdropper is done by a Zigbee radio with a directional antenna. The adaptive secret key extraction scheme is used instead of dropping the mismatched bits with privacy amplification. Multiple bits are extracted in order to increase the secret bit rate. Multi-collision attack which leads to 2n colliding messages after n trails of search is avoided here. The attack can be maintained only if it is a iterative hash function, however it depends up on the actual state. More security has to be provided for reliable communication which is unavailable in the existing systems.

3. ARCHITECTURE DIAGRAM FOR THE PROPOSED SYSTEM


Source
Intermediate
Destination
Send encrypt data and verifies random number from destination
RSS
Receives encrypted data and verifies random number from source
Server
Get and verify username , password and primary key
Get decrypt key and view data

In the existing system, the secret key is generated only by the source and the destination node. The modification that we propose is each and every intermediate nodes generate the secret key that is exchanged with the source for verification. Finally the destination and the source have the same secret key through which the destination can decrypt the data. The intermediate nodes are identified using the Received Signal Strength. RSS is a power signal received by the antenna. The source node finds its next node using the RSS value. The secret key is generated by both the nodes and are exchanged for verification. The source sends the encrypted data to the node and it forwards it to the destination using the destination node's RSS value. After verifying the secret key, the destination node can decrypt the data. In order to increase the output bit stream rate, the hash key of the secret key is generated and is send to the destination.

4. KEY EXTRACTION ALGORITHM

Step 1:
The time series is quantized by each node using specified thresholds by quantization technique.

Step 2:
The initial secret bit stream is divided into several random blocks.

Step 3:
For each block, two adaptive thresholds q+ and q- are calculated such that

$$q+ = \text{mean} + \alpha * \text{std\_deviation} \text{ and}$$
$$q- = \text{mean} - \alpha * \text{std\_deviation} \text{ where } \alpha >= 0.2$$

Step 4:
Adaptive threshold allows the slow shifts in the RSS values.

Step 5:
The RSS measurements above and below the upper and lower threshold values are taken and the values between them are dropped.

Step 6:
The mismatched bits are corrected by using Information Reconciliation technique.

Step 7:
Calculate the Range of RSS measurements from the minimum and the maximum RSS values that are measured.

Step 8:
Find N, the number of bits which can be extracted per measurement,

where $N <= [\log_2 \text{Range}]$

Step 9:
Divide the Range into $P = 2^N$ equal sized intervals

Step 10:
Select an N bit assignment for each p intervals

Step 11: For each RSS measurement, extract N bits that depend on the interval where the RSS measurement lies.

Step 12:
After finishing the above steps, the privacy amplification is used to generate the high entropy secret bit rate.

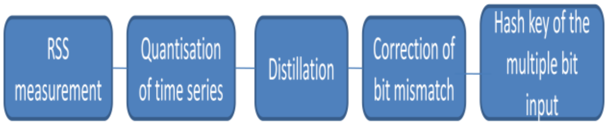

RSS measurement
Quantisation of time series
Distillation
Correction of bit mismatch
Hash key of the multiple bit input

Figure – 1
Stepwise procedure in Secret bit extraction

5. HASH FUNCTION

Step 1:
Fips 180-2 shows the message has a 1-bit appended, and is padded to a whole number of 512-bit blocks, including the message length which is in the 64 bits of the last block.

Step 2:
Since we have only byte-stream instead of a bit-stream, by adding a byte of 10000000 (0x80) appends the bit 1.

Step 3:
To convert this message to 512-bit blocks, calculate the number of required blocks,M. Then for each of these M create a 16 bit array,P. If these are integers, M take four bytes from the data (using char CodeAt), and left-shift them to convert them into the 32-bit integer.

Step 4:
The char CodeAt () method returns NAN for out-of-bounds, but the '|' operator converts this to zero, so the 0-padding is done in a implicit manner.

Step 5:
Then the length of the message has to be appended in the last 64 bits, that is the last two integers of the final block.
M[P-1][14] = ((msg.length-1)*8) >>> 32;
M[P-1][15] = ((msg.length1)*8)&0xffffffff;

Java bit-ops convert their arguments to 32-bits, so n >>> 32 would give 0. For the most-significant 32-bit number, M divide the length by 2^32, and use floor() convert it to an integer.

6. IMPLEMENTATION AND RESULT

We implement the key extraction scheme using information reconciliation, privacy amplification and signal strength on three laptops operating in 802.11g mode. To establish a secret key, the sender and the receiver exchange the probe packets periodically to measure the RSS value. We propose that the source sends a data to the destination; data is forwarded to the intermediate nodes, based on the signal strength. Secret key is generated and is passed by both the source and the destination. A random key is then generated by both source and destination that is exchanged between them for verification. Both of them in turn produce the hash key of the secret keys, which is also verified by them. Only then the Data can be viewed by the Destination. By this we have proposed a strong verification scheme in the destination end. Destination's IP address, Private Key, Random Key, Hash key of Secret Key as well as Secondary Key to change the Primary key is used for the secured communication of data between sender and the receiver. In this security level is highly increased by using the Secret key extraction mechanism. The hash function used here is MNF-256. It is a cryptographic hash function with a message block of 512 bit, 256 bit chaining variables and 512 bit dither value to a hash value of 256 bit. It has three parallel branches each with eight step operations. Preprocessing and computations are the two stages. Message padding, message parsing and initialization of chaining variables are the three sub steps of preprocessing. The experiment was conducted in two different locations where the rate of packet loss rate is calculated. Our experiment revealed that the packet loss rate is more in outdoor than in the indoor.

Table – 1: Rate of packet loss based on distance function

Distance (feet)	Loss rate (Indoor)	Loss rate (Outdoor)
22	1%	2%
48	4%	6%
65	5%	19%
76	6%	22%
94	9%	26%

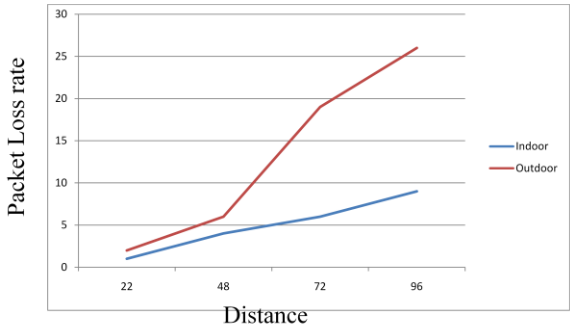


Fig – 2: Comparison of packet loss rate

7. CONCLUSIONS

Thus we have calculated the effectiveness of secret key generation from the measurement of signal strength in a dynamic environment. We have also reduced the generation of predictable key by increasing the rate of secret bits. Further enhancement is done effectively by multiple bit extraction. we then conducted the randomness test. More secure communication is provided by the exchange of random key and hash key of the secret key. Most effective hash function (MNF-256) is used to produce the hash key.

REFERENCES

[1]. Saarinen MO. A meet-in-the-middle collision attack against the new FORK-256 In: INDOCRYPT'07, LNCS, vol. 4859; 2007. P 10–17

[2]. Joux A. Multi-collisions in iterated hash functions. In: CRYPTO'04, LNCS, vol. 3152; 2004. p. 306–16.

[3]. 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.

[4]. 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.
[5]. 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.
[6]. Harshvardhan Tiwari *, Krishna Asawa "A secure and efficient cryptographic hash function based on NewFORK-256" Received 8 June 2012; revised 28 July 2012; accepted 23 August 2012 Available online 29 September 2012
[7]. Abidalrahman Moh'da, Hosein Marzib, Nauman Aslama, William Phillipsa, William Robertsona, a*" A Secure Platform of Wireless Sensor Networks" 1877–0509 © 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of Prof. Elhadi Shakshuki and Prof. Muhammad Younas.