International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 3 479 – 482

A Survey on Secret Key Extraction Using Received Signal Strength in Wireless Networks

Hemavathi M N
Computer Science &Engineering
Vidya Vikas Institute of Engineering & Technology
Mysore, India
hema08.work@gmail.com

Annapurna V K
Computer Science &Engineering
The National Institute of Engineering
Mysore, India
annu_purna_i@yahoo.com

***Abstract*—** Secure wireless communications typically rely on secret keys, which are difficult to establish in an ad hoc network without a key management infrastructure. The channel reciprocity and spatial decorrelation properties can be used to extract secret key, especially in a Rayleigh fading channel. But the intervention of intermediate objects between the communication nodes reduces the strength of the secret key generated through such methods. Furthermore, the impact of small fluctuations also reduces the bit matching rate of such key agreement methods. This paper is based on the survey conducted on secret key generation from Received Signal Strength (RSS). By considering uniqueness property of RSS as base, various authors have proposed different methods for secret key extraction. Due to use of RSS for key extraction the existing systems suffer from predictable filter response at random period. The existing system also faces signal fading and drop in RSS because of intermediate object. By this survey we specify that even after generating high entropy bits for key extraction, there are considerable drawbacks in extracted key due to intervention of intermediate objects and remarkable fading and drop in RSS.

Keywords-- *wireless networks, received signal strength (RSS), multipath fading, cryptography, key generation*

*****

I. INTRODUCTION

The wireless communication revolution is bringing fundamental changes to data networking, telecommunication, and is making integrated networks a reality. By freeing the user from the cord, personal communications networks, wireless LAN's, mobile radio networks and cellular systems, provides fully distributed mobile computing and communications, anytime, anywhere. Secret key generation and establishment is a fundamental requirement for private communication between two entities. Currently, the most common method for generating a secret key in wireless networks is by using some random number or using received signal strength (RSS). Key management infrastructure is basic foundation for secret key establishment in traditional public key cryptography. Since public key cryptography consumes significant amount of computing resources and power, it is not preferred for secret key establishment in wireless networks. The main objective of this paper is to address the problem of secret key generation for securing private communication in public network by comparing the existing methods.

This paper is organized as follows- In section two we present RSS and its components. Section three contains related work on key generation using RSS. Finally, section four gives the comparison of key extraction techniques using RSS and its drawbacks.

II. RECEIVED SIGNAL STRENGTH

Existing secret key extraction in some of the wireless network uses RSS scheme. 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. The RSS can be used as a channel statistic, primarily because of the wireless cards, which can measure RSS on per frame basis without any modification. The variation of RSS over time caused by motion and multipath fading can be quantized and used for generating secret keys. The mean RSS value is somewhat predictable function of distance. This 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.

A less expensive and more flexible solution to the problem of extracting and 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, at some point of time it generates identical filter response for signals sent from Alice to Bob as well signals sent from Bob to Alice. This specifies that identical filter response of RSS will give chance for intruder to predict the pattern. And some frequent problems like signal fading and drop in the RSS caused by intermediate object also degrade the strength of extracted secret key.

A. Components of RSS-Based Secret Key Extraction

To establish a shared secret key, Alice and Bob measure the variations of the wireless channel between them across time by sending probes to each other and measuring the RSS values of the probes. Ideally, both Alice and Bob should measure the RSS values at the same time. Typical commercial wireless transceivers are half duplex, i.e., they cannot both transmit and receive the signals simultaneously. Thus, Alice and Bob must measure the radio channel in one direction at a time. However, as long as the time between two directional channel measurements is much smaller than the inverse of the rate of change of the channel, they will have similar RSS estimates.

Most of the existing literature on key extraction from RSS measurements either use some or all of the following three steps:

A.1 Quantization

As multiple packets are exchanged between Alice and Bob, 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 thresholds. Figure 1 shows a sample RSS quantizer with two thresholds. The values between the lower and upper threshold are dropped, the value greater than the upper threshold is encoded as 1 and the value less than the lower threshold is encoded as 0. For the example in figure 1 the quantizer will output 1010011. Different quantizers have been proposed in the existing systems [5], [6], [20], [24]. The difference in these quantizers mainly results from their different choices of thresholds and the different number of thresholds that they use.

A.2 Information Reconciliation

The existing system use Cascade an interactive information reconciliation protocol. In this protocol, Alice permutes the bitstream randomly, divides it into small blocks and sends permutation and parity information of each block to Bob. Bob permutes his bitstream in the same way, divides it into small blocks, and computes parities and checks for parity mismatches.

A.3 Privacy Amplification

It is observed that the information reconciliation stage reveals a certain fraction of information to correct the mismatching bits of Alice and Bob. The leaked portion needs to be removed so that an adversary cannot use this information to guess portions of the extracted key. Privacy amplification solves the above two problems by reducing the size of output bit stream. This is achieved by letting both Alice and Bob use universal hash functions. These functions are randomly chosen from a publicly known set, to obtain fixed size smaller length output from longer input streams. Essentially, privacy amplification generates a shorter secret bit stream with a higher entropy rate and a longer secret bit stream with a lower entropy rate. Most of the popular methods used for privacy amplification are based on the *leftover hash lemma*, a well known technique to extract randomness from imperfect random sources.

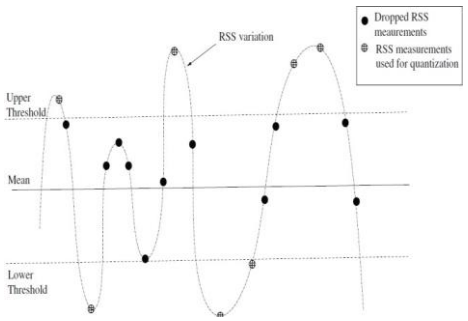

Figure. 1 A sample RSS quantizer

III. RELATED WORK

Several researchers have proposed to use the unpredictability of the radio channels to extract secret keys. The level-crossing method [20] uses a protocol that allows two users to establish a common cryptographic key by exploiting special properties of the wireless channel. The underlying channel response between any two parties is unique and decorrelates rapidly in space. The established key can then be used to support security services (such as encryption) between two users. The algorithm here uses quantization along with level-crossing to extract bits from correlated stochastic processes. The resulting protocol resists cryptanalysis by an eavesdropping adversary and a spoofing attack by an active adversary without requiring an authenticated channel.

Another author proposed a improved level-crossing [25] approach, which is well-suited for the Rayleigh and Rician fading models associated with a richly scattering environment for building practical secret key generation protocols between two entities. This level-crossing algorithm is simple, and incorporates a self-authenticating mechanism to prevent adversarial manipulation of message exchanged during the protocol.

A different approach [19] is used for generation of the shared key in some existing system, where the transceivers use Low Density Parity Check (LDPC) decoders to resolve the differences in their channel impulse response measurements caused by noise. To ensure secret key agreement, a method of public discussion between the two users is performed using the syndrome from Hamming (7,3) binary codes. This algorithm checks the equality of generated keys for both legitimate users, and ensures error-free secure communication

 ISSN: 2321-8169
479 – 482

Later Adaptive Secret Bit Generation (ASBG) [17] evaluated the effectiveness of secret key extraction, for private communication between two wireless devices. Using real world measurements of RSS in a variety of environments and settings, secret key was extracted from RSS variations on the wireless channel. The ASBG approach generated bit streams of High entropy. The quantizer used in this method divides the RSS measurements into smaller blocks of *block size* and calculates the thresholds for each block separately. The adaptive threshold allows the quantizer to adapt to slow shifts of RSS.

All the above schemes provided the best method of extracting the secret key from the RSS in the wireless network configurations. But RSS suffers from predictable filter response at random period, signal fading and drop because of intermediate object.

IV. COMPARISION

In this section we compare two well known methods for extracting secret key from RSS. To determine the effectiveness in a wireless environment, the existing systems implemented the two most relevant methods, level crossing [5] and Adaptive Secret Bit Generation (ASBG) [7].

A. Level crossing: overview and limitations

Level crossing consists of two steps. First, Alice and Bob keep probing the channel and collecting RSSI readings. They map each reading to a temporary bit as follows. Consider the case for Alice.

Let μx be the mean of X,

σx be the standard deviation.

Each reading x is mapped to a temporary bit via a quantizer Q such that

Q(x)=1 if x > q+;

Q(x) =0 if x < q-;

Q(x) =e, otherwise, where e is a undefined state and

q+ = μx + σx,

q-= μx –α σx where α is a parameter to be tuned.

This can be seen in Figure 2. Bob's quantizer is similar. Second, Alice and Bob communicate to get final bits from temporary bits. They identify excursions in temporary bits. An excursion is a consecutive of 1s or 0s with length at least m where m is the second parameter to be tuned. For example, if the temporary bits are "e0000111e111e" and m = 3, then there are 3 excursions: e {0000}{111}e{111}e. Alice finds from her temporary bits all excursions, and sends the indexes of all excursion centers to Bob.

On receiving the indexes, Bob checks each index to see whether he also has an excursion around this index, and sends the result back to Alice. Finally, they quantize each common excursion to a bit. For the above example, if Bob has the same temporary bits, then they both get 011. The name of final bits (a bit vector) as quantized bits. The bits at Alice and Bob may be different. Each different bit is a mismatch. The ratio of the number of mismatches and the number of quantized bits is defined as mismatch rate. The level crossing algorithm subtracts a windowed moving average from the raw data to reduce the influence of slow variation, where the output of the sliding window is the slow variation. This creates the third parameter: the window size s. The residuals, rather than the raw readings, are fed into the quantizer Q. In summary, we have three parameters: reading threshold, excursion threshold m, and window size s.

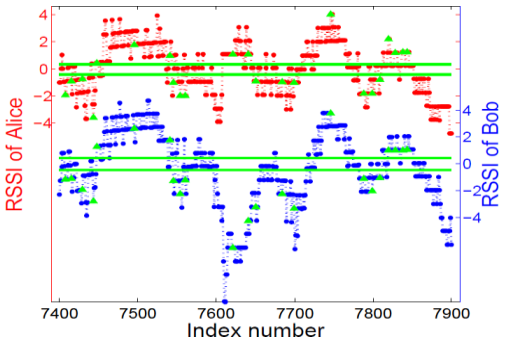

Figure.2 Level crossing on a portion of residuals. The two lines for Alice(top) or Bob(bottom) are the q+,q- in quantizer Q, and each triangle corresponds to a quantized bit.

This experiment finds that the generic level crossing method can result in low mismatch ratio. However, directly applying level crossing is not sufficient to achieve good bit rate. Therefore, improvements on the generic level crossing methods took place. Even though level crossing is a groundbreaking approach to secret extraction, it has some questions that are not answered. Applying it to wirelesstrace shows the following problems.

- It causes mismatches which seriously influence the variations on performance in highly noisy environments.
- There are no guidelines to select parameters for level crossing.
- The level crossing scheme does not estimate the randomness of the generated bit string nor does it generate a bit string that is necessarily random
- The level crossing scheme uses a fixed set of parameters, which does not adapt to the drastic change of channel dynamics in wireless environments.

B. *Adaptive Secret Bit Generation: overview andlimitations*

One more existing method for secret key extraction is Adaptive Secret Bit Generation to generate bit streams of High entropy. The quantizer used in this method divides the RSS measurements into smaller blocks of *block size* and calculates the thresholds for each block separately. The adaptive threshold allows the quantizer to adapt to slow shifts of RSS. 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 (for example the Graycode sequence), and
(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.

This single bit extraction in conjunction with information reconciliation and privacy amplification is able to achieve higher entropy in comparison to level crossing schemes, and allows significant increase in the secret bit rate as well. But the variation of RSS over time caused by motion and multipath fading can be quantized and used for generating secret keys. The mean RSS value is somewhat predictable function of distance. This 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 they are 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 secret bits between Alice and Bob.This specify that identical filter response of RSS will give chance for intruder to predict the pattern. Some frequent problems like signal fading and drop in the RSS caused by intermediate object also degrade the strength of extracted secret key.

CONCLUSION

We compared the effectiveness of secret key extraction from the received signal strength (RSS) variations in wireless channels. Our survey conclude that bits extracted in wireless environments using RSS are unsuitable for generating a secret key, because of static nature of level crossing in selecting parameters. Even though level crossing is a revolutionary approach to secret key extraction, parameter selection, estimation of randomness causes barrier to dynamicity of extraction process. In ASBG generation of predictable filters response at random period, signal fading and drop in RSS because of intermediate object influences limitations for strength of extracted secret key. Even though ASBG method generates bit streams of High entropy, this approach could not with stand predictable filter response at random period, signal fading and drop in RSS.

REFERENCES

[1] 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.

[2] ipwraw, http://homepages.tu-darmstadt.de/ p larbig/wlan/.

[3] radiotap, http://www.radiotap.org.

[4] Converting signal strength percentage to dbm values, http://www.wildpackets.com/elements/whitepapers/Converting Signal Strength.pdf.

[5] 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 Transactions on Antennas and Propagation*, 53(11):3776-3784, Nov. 2005.

[6] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In *ACM CCS*, 2007.

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *J. Cryptol.*, 5(1):3-28, 1992.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6):2515-2534, 2008.

[9] G. Brassard and L. Salvail. Secret key reconciliation by public discussion. *Lecture Notes in Computer Science*, 765:410-423, 1994.

[10] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *MOBICOM*, 2008.

[11] G. D. Durgin. *Space-Time Wireless Channels*. Prentice Hall PTR, 2002.

[12] L. Greenemeier. Election fix? switzerland tests quantum cryptography. *Scientific American*, October 2007.

[13] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu. Cryptographic key agreement for mobile radio. *Elsevier Digital Signal Processing*, 6:207–212, 1996.

[14] J. E. Hershey, A. A. Hassan, and R. Yarlagadda. Unconventional cryptographic keying variable management. *IEEE Trans. Commun.*, 43(1):3-6, Jan. 1995.

[15] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *STOC*, pages 12-24, 1989.

[16] S. Jana and S. K. Kasera. On fast and accurate detection of unauthorized access points using clock skews. In *MOBICOM*, 2008.

[17] 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. In *ACM MOBICOM*, 2009.

[18] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via lower layer enforcements. In *ACM WiSe*, 2006.

[19] M. G. Madiseh, M. L. McGuire, S. W. Neville, and A. A. B. Shirazi. Secret key extraction in ultra wideband channels for unsynchronized radios. In *CNSR*, May 2008.

[20] S. Mathur, W. Trappe, N. B. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *ACM MOBICOM*, 2008.

[21] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Info. Theory*, 39(3):733-742, May 1993.

[22] U. M. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Trans. Info. Theory*, 45(2):499-514, 1999.

[23] A. Sayeed and A. Perrig. Secure wireless communications: Secret keys through multipath. In *ICASSP*, pages 3013-3016, April 2008.

[24] M. A. Tope and J. C. McEachen. Unconditionally secure communications over fading channels. In *MILCOM*, 2001.

[25] Chunxuan Ye, Suhas Mathur, Alex Reznik, Yogendra Shah, Wade Trappe, and Narayan B. Mandayam, IEEE transactions on information forensics and security, vol. 5, no. 2, june 2010