Secret Key Extraction for Wireless Networks During Data Transmission

[1]S. Vijayasivaraman, [2]R. Satheeskumar, [3]B. Anbuselvan

[1]Department of Computer Science, Bharath Niketan Engineering College
[2]Head of the Department Computer Science and Engineering, Bharath Niketan Engineering College
[3]Assistant Professor Computer Science and Engineering, Bharath Niketan Engineering College
[1]*csvijaysmns@gmail.com*

Abstract**--**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. Our experimental results show that (i) in certain environments, due to lack of variations in the wireless channel, the extracted bits have very low entropy making these bits unsuitable for a secret key, (ii) an adversary can cause predictable key generation in these static environments, and (iii) in dynamic scenarios where the two devices are mobile, and/or where there is a significant movement in the environment, high entropy bits are obtained fairly quickly.. Our measurements show that our scheme, in comparison to the existing ones that we evaluate, performs the best in terms of generating high entropy bits at a high bit rate. The secret key bit streams generated by our scheme also pass the randomness tests of the NIST test suite [1] that we conduct. We also build and evaluate 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, we evaluate secret key extraction in a multiple input multiple output (MIMO)-like sensor network testbed that we create using multiple TelosB sensor nodes. We find that our MIMO-like sensor environment produces prohibitively high bit mismatch, which we address using an iterative distillation stage that we add to the key extraction process. Ultimately, we show that the secret key generation rate is increased when multiple sensors are involved in the key extraction process.

Keywords*- Wireless networks, multipath fading, physical layer, cryptography, key generation.*

*****

1. INTRODUCTION

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. 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. Quantum cryptography is a good example of an innovation that does not use public keys. It uses the laws of Quantum theory, specifically Heisenberg's uncertainty principle, for sharing a secret between two end points. Although quantum cryptography applications have started to appear recently , they are still very rare and expensive.

Aless expensive and more flexible solution to the 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. 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 nonideal 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.

Azimi-Sadjadi et al. suggested using two well-known techniques from quantum cryptography information reconciliation and privacy amplification, to tackle the challenge caused by RSS measurement asymmetry. Information reconciliation techniques (e.g., Cascade [9]) leak out minimal information to correct those bits that do not match at Alice and Bob. Privacy amplification reduces the amount of information the attacker can have about the derived key. This is achieved by letting both Alice and Bob use universal hash functions, chosen at random from a publicly known set of such functions, to transform the reconciled bit stream into a nearly perfect random bit stream.

Most of the previous research work on RSS-based secret key extraction, including that of Azimi-Sadjadi et al. , is based on either simulations or theoretical analysis. Other than the recent work by Mathur et al. 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. We 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. In order to perform our measurements and subsequent evaluations, we implement different RSS quantization techniques in conjunction with information reconciliation and privacy amplification.

We first collect measurements under different environments to generically evaluate the effectiveness of secret key generation. We find that under certain environments due to lack of variations in the channel, the extracted key bits have very low entropy making these bits unsuitable for a secret key. Interestingly, we also find that an adversary can cause predictable key generation in these static environments. However, in scenarios where Alice and Bob are mobile, and/or where there is a significant movement in the environment, we find that high entropy bits are obtained fairly quickly. Next, building on the strengths of the existing schemes, we develop an environment adaptive secret key generation scheme that uses an adaptive lossy quantizer in conjunction with Cascade-based information reconciliation and privacy amplification. Our measurements show that our scheme performs the best in terms of generating high entropy bits at a high bit rate in comparison to the existing ones that we evaluate. The secret key bit streams generated by our scheme also pass the randomness tests of the NIST test suite that we conduct We also build and evaluate 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. Finally, we also evaluate secret key extraction in a multiple input multiple output (MIMO)- like sensor network testbed that we create using multiple TelosB sensor nodes. We find that our MIMO-like sensor environment produces prohibitively high bit mismatch, which we address using an iterative distillation stage that we add to the key extraction process. Ultimately, we show that the secret key generation rate is increased when multiple sensors are involved in the key extraction process.

2 ADVERSARY MODEL

In our adversary model, we assume that the adversary Eve can listen to all the communication between Alice and Bob. Eve can also measure both the channels between herself and Alice and Bob at the same time when Alice and Bob measure the channel between themselves for key extraction. We also

assume that Eve knows the key extraction algorithm and the values of the parameters used in the algorithm. However, we assume that Eve cannot be very close (less than a few multiples of the wavelength of the radio waves being used to either Alice or Bob while they are extracting their shared key. This will ensure that Eve measures a different,

uncorrelated radio channel We assume that Eve can

neither jam the communication channel between Alice and Bob nor can she modify any messages exchanged between Alice and Bob. Essentially, Eve is not interested in disrupting the key establishment between Alice and Bob. However, in our model Eve is free to move intermediate objects between Alice and Bob and affects their communication channel

although we assume that Eve is unable to restrict other movements in the channel and thus will not be able to significantly increase the coherence time of the channel. We also assume that Eve cannot cause a person-in-the-middle attack, i.e., our methodology does not authenticate Alice or Bob. In other words, our proposed scheme works against passive adversaries. Even without an authentication mechanism, the Diffie-Hellman secret key establishment scheme has found widespread use in network security protocols and standards (e.g., for providing Perfect Forward Secrecy, Strong password protocols, etc.). We expect that our scheme will provide a strong alternative to the Diffie Hellman scheme in wireless networks. There is a growing amount of work in authenticating wireless devices based on their physical and radiometric properties . These and future authentication mechanisms can be used in conjunction with our secret key establishment scheme.

3. METHODOLOGY

In this section, we first describe the three components of our wireless RSS-based secret key extraction. Next, we briefly describe two classes of existing quantization approaches. Last, we develop a new approach by combining the advantages of the existing approaches.

3.1 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. However, typical commercial wireless transceivers are half duplex, i.e., they cannot both transmit and receive the signals simultaneously. Thus, Alice and Bob must measure

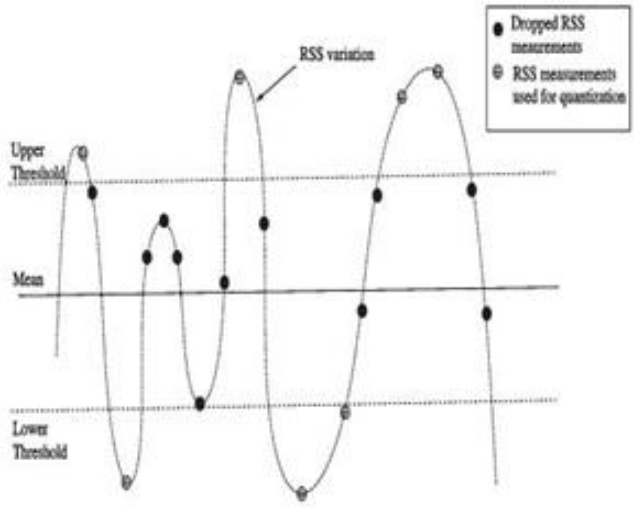


Fig 3.1

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.

3.1.1 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. Fig. 1 shows a sample RSS quantizer with two thresholds. Different quantizers have been proposed in the existing literature The difference in these quantizers mainly results from their

different choices of thresholds and the different number of thresholds that they use.

3.1.2 Privacy Amplification

When the probe packets are exchanged at a rate greater than the inverse of the coherence interval of the channel, there may be short-term correlation between subsequent quantized bits. Moreover, 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, chosen at random from a publicly known set of such functions, 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 from 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 .We implement this technique in this paper.

3.2 Existing Approaches

We classify the existing approaches into the following t wo categories:

Lossy-quantization-based approach: In this approach,

bits extracted from the RSS measurements are ropped probabilistically to maintain a high bit entropy. This approach does not use privacy amplification. The goal of this approach is to output a high entropy bit stream so that the output bit stream can be used directly as the shared secret key. This approach has a low output bit rate. Examples of this approach include quantization methods of Aono et al. Tope and McEachen , and Mathur et al. . Lossless-quantization-based approach: This approach does not drop any bits but uses privacy amplification to increase the bit entropy. This approach produces a high rate output bit stream (e.g., Azimi-Sadjadi et al.'s method .Note that quantization is inherently lossy. However, in this paper lossless quantization corresponds to obtaining 1 bit or more per sample and lossy quantization corresponds to obtaining less

than 1 bit per sample. Also note that we compare these different approaches for the quality of the bit streams they generate. This quality is quantified by three performance metrics:

3.2.1. Entropy: Entropy characterizes the uncertainty associated with a random variable. We estimate the entropy of a bit stream using NIST test suite's Approximate entropy test.

3.3.2. Bit mismatch rate: We define the bit mismatch rate as the ratio of the number of bits that do not match between Alice and Bob to the number of bits Extracted from RSS quantization.

3.3.3 Secret bit rate: 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.

3.3 Adaptive Secret Bit Generation (ASBG)

Our experimental results in Section 5 suggest that some lossy quantizers like Aono et al.'s quantizer or Tope et al.'s quantizer that aim to achieve high bit rate can output bit streams with low entropy in certain settings, especially in those that have minimal movement. On the other hand, some other lossy quantizers like Mathur et al.'s quantizer, can output bit streams with reasonably high entropy but sacrifice the bit rate to achieve this or vice versa. The lossless quantizer described above also generates secret bits at a low rate. In summary, the existing approaches that use RSS measurements do not generate secret bits at a high rate and/or with high entropy. We develop a method, that we call ASBG, that builds on the strengths of the existing approaches. In our method, we use a modified version of Mathur's quantizer in conjunction with two well-known information reconciliation and privacy amplification techniques.

Various single bit quantization methods drop a large amount of RSS samples that lie in between the upper and lower thresholds. These dropped samples constitute a loss of valuable information that can be used by Alice and Bob to generate secret bits and also result in an inefficient utilization of the wireless medium because more probes must be sent and received. Furthermore, privacy amplification also reduces the secret bit rate while increasing entropy. To increase the secret bit rate, we propose an adaptive scheme for extracting multiple bits from a single RSS measurement. Our multiple bit extraction scheme is described as follows. 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 <[log2] Range,
3. divide the Range into M (power 2N)equal sized intervals,
4. choose an N bit assignment for each of the M intervals (for example, use the Gray code sequence
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 of reconciliation to correct the mismatching bits, and finally, apply privacy amplification to the reconciled bit stream and extract a high entropy bit stream. Our results, as presented in Section 6, 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 enhancement (evaluated in Section 7) allows us to significantly increase the secret bit rate as well.

4. IMPLEMENTATION

We implement the key extraction scheme consisting of three components, namely quantization, formation reconciliation, and privacy amplification, on two laptops (Alice and Bob) equipped with in-built Intel PRO/Wireless 3,945 ABG wireless network cards, operating in the 802.11g mode. Both laptops run the Ubuntu Linux operating system. In order to establish a secret key, Alice and Bob exchange probe packets periodically and use these probe packets to measure the RSS values.

4.1 MODULES

- Network construction
- Server
- Encryption
- Key generation based on rss
- Random number generation
- Prinary key and master key and authentication

4.1.1 NETWORK CONSTRUCTION:

To implement the Project concept, first we have to construct a network which consists of 'n' number of Nodes. So that nodes can request data from other nodes in the network. Since the Nodes have the mobility property, they can move across the network. To show this concept we'll create the Node frame which contains the time. Based on the time change we can assume that the nodes are moving across the network. For each node we have to create a Node Frame which contains the Node information, Destination Node field to transfer the data and the browse button to upload the data from Node's directory.

4.1.2 SERVER:

A server is a computer program running to serve the requests of other programs, the "clients". Thus, the "server" performs some computational task on behalf of "clients". The clients either run on the same computer or connect through the network. Server is the module which is used to store all the Nodes information like Node Id, Password, IP address and other information in its database. Also the Server will monitor all the Nodes Communication for security purpose.

4.1.3ENCRYPTION:

If the Source nodes wants 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.

4.1.4 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.

4.1.5RANDOM 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.

4.1.5 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 these information are 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.

5. DISTILLATION (Algorithm)

To address the problem of very high bit mismatch rates, we augment the secret key extraction process with the distillation stage. Distillation ensures that the percentage of mismatching bits is low enough for information reconciliation to correct the differences without revealing all the extracted bits. Fig. 16 shows the distillation stage in relation to the other stages of the key extraction process. Plotting the measurements from channels with large channel distances, we find that a large fraction of consecutive measurements exhibit abrupt transitions from one quantization level to another resulting in asymmetry. The distillation stage seeks to iteratively eliminate such measurements causing abrupt transitions. If the mismatch is still too high even after one round of eliminations, it is necessary to eliminate further; in which case, the next best elimination candidates are those that follow the previously eliminated measurements. When this process is iterated over a number of times, it is guaranteed to improve the bit mismatch rate. Note that the number of iterations required depends on the current expected mismatch rate of the channel, which can be determined based on the history of mismatch rate of the channel. the actual bit pattern assigned to each interval. Exclude label is a special label indicating an eliminated measurement. Thus, despite the simplicity of the distillation approach, these results show that it can reduce the bit mismatch rate very effectively.

Algorithm 1 succinctly expresses the steps taken in each iteration. Essentially, in a given block of at leasti quantization labels, which are identical (e.g., consecutive as), iteration number removes the prefix of length i from that block; in case the block length is less than i, it removes the entire block.

Algorithm 1.Distill Input

```
While there is input do
if current_label =previous_label then
Output current _label
else
Output excludes _label
Previous _label⟸ current _label
end if
end while
```

5.1PROHIBITIVELY HIGH BIT MISMATCH

When using multiple sensors, we find that the bit mismatch rate is significantly higher in comparison to our earlier experiments that use 802.11 single antenna systems. Note that for a mismatch rate of about 22 percent, the information reconciliation protocol essentially reveals all the bits. So, the collected measurements that exhibit very high bit mis match are not useful in establishing a secret key.

We identify the following reasons for such high mismatch rates. First, when multiple nodes take turn in exchanging probe packets, it increases the average time gap between any pair of measurements taken in each direction of a channel, and also reduces the probing rate on each channel. Both these factors contribute in increasing the bit mismatch rate. This is also verified in a plot of bit mismatch rate versus channel distance, where channel distance is the absolute difference between the node ids (as defined by the token ring order) of the transmitting and Receiving sensors. Learly shows the general increase in mismatch rate with channel distance. Time gap between each unidirectional measurement pairs is

proportional to the channel distance. So, mismatch rate increases with channel distance/multiple antennas. Second, channels in 802.15.4 are much narrower in comparison to 802.11. Nonreciprocal's deep fade (perhaps due to strong interference only at Alice) occurring on a narrow channel significantly reduces the average RSS computed at Alice while not affecting much at Bob. This results in a greater likelihood of asymmetry in measurements, and therefore higher bit mismatch when using narrow channel measurements.

6. SYSTEM MODEL

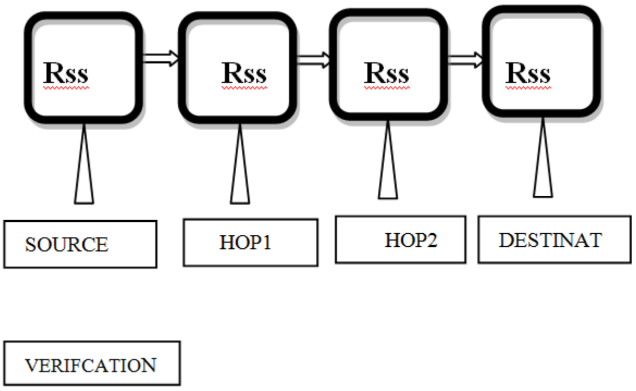


Fig 6.1

Fig 6.1 shows part of an ad hoc network. Some nodes in the ad hoc network may have wireless interfaces to connect to the wireless infrastructure such as wireless LAN or cellular networks. Suppose node N11 is a data source (center), which contains a database of n items d1; d2; . . . ; dn. Note that N11 may be a node connecting to the wired network which has the database. In ad hoc networks, a data request is forwarded hop-by hop until it reaches the data center and then the data center sends the requested data back. Various routing algorithms have been designed to route messages in ad hoc networks. To reduce the bandwidth consumption and the query delay, the number of hops between the data center and the requester should be as small as possible. Although routing protocols can be used to achieve this goal, there is a limitation on how much they can achieve. In the following, we propose two basic cooperative caching schemes

6.1.1 Secret Key Extraction Using Handheld Devices

Given the widespread prevalence of inexpensive and low power mobile devices, in this section, we evaluate our secret key extraction using two mobile devices,

Google Nexus One smart phones, that are equipped with Broadcom BCM 4329 chipset-based 802.11 wireless network cards. We first perform experiments similar to the ones described in the previous section in two different environments.

Although not shown here, we obtain high entropy secret bits fairly quickly when using these smart phones and our secret bit streams also pass the NISTs approximate entropy test, achieving an entropy value close to the ideal value of one. In the rest of this section, we examine the impact of distances between two smart phones, Alice and Bob, on secret key extraction in two different environments while they transmit at a very low power

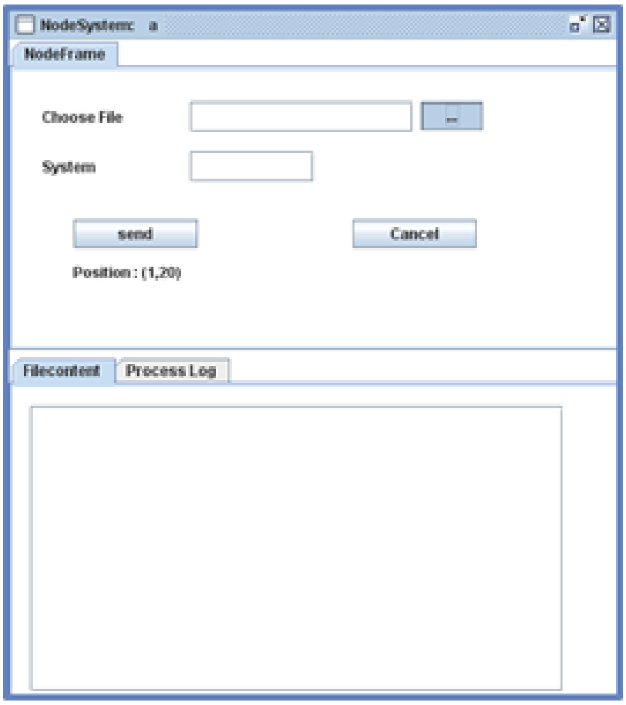


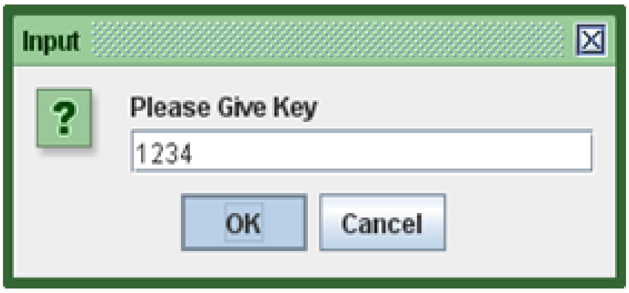
Fig 6.2

6.1.2Experimental Setup

We conduct a number of experiments in the University of Utah campus under two different environments that are changing with time. In each environment, we perform four walk-experiments where the phones representing Alice and Bob are carried at normal walking speeds. (Fig 6.2)The average distance (d) in feet between Alice and Bob is varied with each experiment andd2f25;50;75;100g This first environment is a hallway on the third floor of the Merrill Engineering building. In the experiments conducted in this environment, our phones use the lowest transmit power of 4 dBm. We conduct a second set of experiments in an outdoor environment across varying terrain, with many trees and bushes in the path between Alice and Bob. Because of the terrain and obstructions in this environment, the path losses are higher. Due to greater path loss in this environment, we use a higher transmit power of 8 dBm

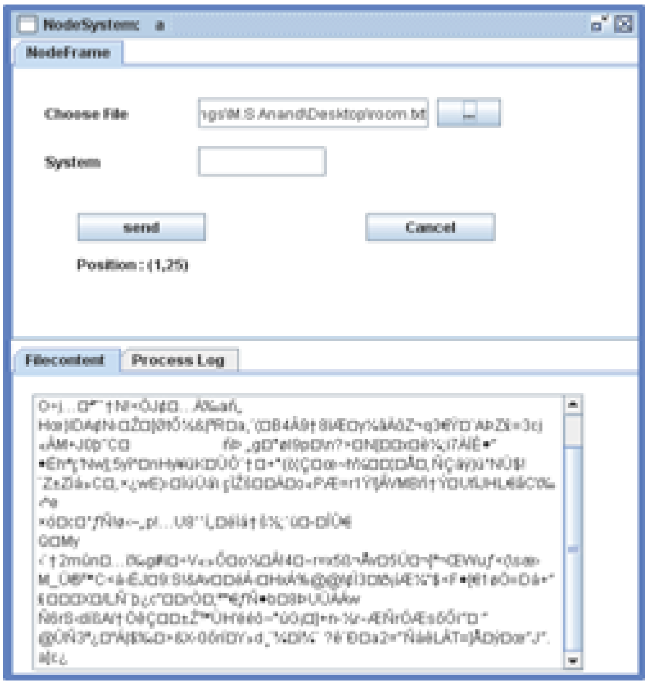
6.1.3 PERFORMANCE EVALUATION

In this section, we evaluate secret key extraction as a function of distance between Alice and Bob. Our results show that in the hallway environment(fig 6.3), even with the lowest transmit power, Alice and Bob can extract about 0.25 secret bits per probe when they are separated by about 25 feet .



Please Give Key
1234

Fig 6.3



Choose File ngs\M.S Anand\Desktop\room.txt
System
Position : (1,25)

Fig 6.4

Fig. 6.1 shows a plot of secret bits per probe as a function of the distance between Alice and Bob. Though we use a lower transmit power in the hallway environment, in comparison to the trees environment, the hallway environment achieves a higher performance due to lower signal attenuation from our measurements, we find that for a given distance, the average received powers are about 2-7 dB higher in the hallway environment in comparison to the obstructed outdoor environment. As we show in Fig. 14, secret bits per probe decreases with increase in distance, which is attributed to the following reason: As the distance increases the signal-to-noise ratio (SNR) decreases, which consequently increases both the bit mismatch rate and the packet drop probabilities ; the increase in packet drop further contributes to an increase in the time duration between channel measurements. Nevertheless, on the whole, a comparison of our results in Figs. 6.4 Shows that secret keys can be established efficiently even with low-powered, mobile devices

7. CONCLUSION AND FUTURE WORK

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. Th 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 test bed 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.

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.tudarmstadt.de/p_larbig/wlan, 2012.

[3] "Radiotap," http://www.radiotap.org, 2012.

[4] "Converting Signal Strength Percentage to dBm Values,"http://www.wildpackets.com/elements/whitepapers/Converting Signal_Strength.pdf, 2012.

[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 Trans. Antennas and Propagation,vol. 53, no. 11, pp. 3776-3784, Nov. 2005.

[6] 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.

[7] 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.

[8] 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

[9] 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.

[10] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures,"Proc. ACM MobiCom, 2008.

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

[12] L. Greenemeier, "Election Fix? Switzerland Tests Quantum Cryptography,"Scientific Am.,Oct. 2007.

[13] A.A. Hassan, W.E. Stark, J.E. Hershey, and S. Chennakeshu, "Cryptographic Key Agreement for Mobile Radio,"Elsevier Digital Signal Processing,vol. 6, pp. 207-212, 1996.

[14] 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.

[15] R. Impagliazzo, L.A. Levin, and M. Luby, "Pseudo-Random Generation from One-Way Functions,"Proc. 21st Ann. ACM Symp. Theory of Computing (STOC),pp. 12-24, 1989.

[16] S. Jana and S.K. Kasera, "On Fast and Accurate Detection of Unauthorized Access Points Using Clock Skews,"Proc. ACM 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,"Proc. ACM MobiCom,2009.

[18] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing Wireless Systems via Lower Layer Enforcements,"Proc. Fifth ACM Workshop Wireless Security (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," Proc. Sixth Ann. Comm. Networks Services Research Conf. (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,"Proc. ACM MobiCom,2008.

[21] 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

Mr.R.Satheeskumar received his B.E. and M.Tech. degree in Computer Science and Pursuing his Phd from Anna University . He is currently working as Head of the Department of Computer Science and Engineering at Bharath Engineering college , Madurai, India. His areas of interest are Data Mining, Software Engineering and Computer Networks, Wireless Sensor Networks. Currently he has published many papers in national and International journals. He is the lifetime member of ISTE and IEEE

Mr.B.Anbuselvan received his M.E. degree in Computer Science and Engineering and Pursuing his Phd from Anna University. He is currently working as Assistant Professor Department of Computer Science and Engineering at Bharath Engineering college , Madurai, India. His areas of interest are Software Testing ,Software Engineering and Computer Networks.DataStructures and Algorithms. Currently he has published many papers in national and International journals. He is the lifetime member of ISTE and IEEE.

Mr.S.Vijayasivaraman received his B.E degree in Computer Science and Engineering and Pursuing his M.E from Anna University.His areas of interest are Mobile computing ,Software Engineering and Computer Networks. . Currently he published many papers in national and international conferences . He is the member of ISTE.