Secret Key Generation Based on Channel and Distance Measurements

Ahmed Badawy*†, Tamer Khattab†, Tarek ElFouly‡, Amr Mohamed‡, and Daniele Trinchero*
*Politecnico di Torino, DET - iXem Lab. (ahmed.badawy, daniele.trinchero@polito.it)
†Qatar University, Electrical Engineering Dept. (tkhattab@qu.edu.qa)
†Qatar University, Computer Engineering Dept. (tarekfouly,amrm@qu.edu.qa)

***Abstract*—Within the paradigm of physical layer secrecy, typically a physical layer specific characteristic is used as key generator to guarantee information hiding from eavesdroppers. In this paper, we propose a novel secret key generation algorithm based on two reciprocal physical layer parameters; the channel measurements and the distances between the two communicating nodes. The two parameters are estimated experimentally using implementations of our algorithm on three FPGA- based WARP kits emulating the two communicating nodes and the eavesdropper. The parameters are used as common sources of randomness to generate the secret key. We evaluate the performance of our algorithm through extensive iterations. We compare the bit mismatch rate as well as the entropy of the generated secret key of our algorithm versus classical channel only and distance only based algorithms. Our results reveal that even in the worst case scenarios, our algorithm outperforms the two other algorithms and overcomes their vulnerabilities.**

***Index Terms*—Channel Estimation, Secret Key, Localization, Bit Mismatch Rate.**

I. Introduction

One well known characteristic of the communication channel is reciprocity. When two antennas communicate by radiating the same signal through a linear and isotropic channel, the received signals by each antenna will be identical. This is mainly because of the reciprocity of the radiating and receiving antenna pattern [1].

Current physical layer security techniques are based on channel reciprocity assumption. The most common feature of the channel characteristics that is widely used is channel amplitude; mainly because of its ease of implementation [2]–[5]. The authors in [6] developed a level crossing algorithm that is best suited for Rician and Rayleigh fading [6]. The ultrawideband channel impulse response is used in [7] as the source of common randomness. In [8], the authors developed a technique to transform correlated channel measurements into uncorrelated binary data. Other reciprocal (common) parameters such as received signal strength (RSS) can be used as a common source of randomness to generate the secret key [9].

A recent physical layer security technique that is based on the distance reciprocity to generate secret key bits is presented in [10], [11]. Their work is based on [12], which studies the problem of generating a secret key from common randomness shared between the intended nodes. The motivation behind the authors work is that the current techniques, which exploit the channel gain, are based on the assumption that the channel gains are independent of the distance. This assumption could be valid for non-line of sight fading channel but not necessarily a valid assumption for line of sight fading channel where attenuation is a function of the propagation distance. In this case, an eavesdropper with localization or distance estimation capabilities can then estimate the channel gain and consequently recover the secret key. Examples of localization techniques can be found in [13], [14]. There are other techniques to perform localization which are based on the time of arrival (TOA) [15]–[18]. Angle of arrival (AOA) can also be used for localization as shown in [14], [19]. RSS is a very common metric that requires a simple circuitry to be implemented. Exploiting the RSS to estimate the distance is presented in [20], [21].

The authors in [11] did not consider that the secret key generated based on the distance between the two communicating nodes is susceptible to be recovered by an eavesdropper that is equipped with AOA estimation capabilities. In this case, the eavesdropper estimates the AOA for both the signal received from the two nodes as well as the the distances between itself and the two nodes. The eavesdropper then easily estimates the distance between the two nodes. Once the distance between the nodes is estimated, the secret key is recovered by the eavesdropper.

To address this latter drawback, we propose a novel algorithm that exploits a combination of the channel gain as well as the distance between the two nodes as a joint (hybrid) common source of randomness. Our algorithm is well suited for both line of sight and non line of sight channel, which overcomes the drawback of the distance based algorithms as well as the channel gain algorithm.

Our contributions in this work as compared to available literature are as follows: We propose a new physical layer based secret key generation algorithm which is based on joint common sources of randomness stemming from distance and channel gain between the trusted nodes. We implement the crucial parts of our algorithm on a prototyping platform to demonstrate its practicality and to collect measurements for performance evaluation. We compare our results with existing single source based algorithm to show the advantages of our hybrid technique. To the best of the authors' knowledge, exploiting two common sources of randomness has not been studied yet. Exploiting a second source of randomness adds a degree of freedom to the trusted nodes in case each common

source or randomness can be estimated by the eavesdropper.

The rest of this paper is organized as follows: In Section II the adversary model is presented. The channel gain measurements is then addressed in section III. We then use the RSS to estimate the distance in Section IV. Our secret key generation algorithm is presented in Section V. We evaluate the performance of our algorithm in Section VI. The paper is then concluded in section VII.

II. Adversary Model

In our adversary model, we assume that an eavesdropper (Eve) can listen to all the communications between the two trusted communicating nodes (Alice) and (Bob). Eve can estimate the channel gains between itself and both Alice and Bob. In addition, it can estimate the distances between itself and Alice and Bob. We also assume that Eve's radio might be equipped with AOA estimation capabilities, hence it can estimate the AOA for both signals received from Alice and Bob. In our model, Eve can move freely within the field and can visit any of the locations where either Alice or Bob were or will be in the future. Eve can not be within a few wavelength near to either Alice or Bob to ensure that the collected signals are not correlated. We assume that Eve is not interested in denial of service attack, person in the middle attack or jamming attack. Rather, we assume that Eve is a passive adversary.

III. Channel Gain Measurements

As stated earlier, the channel amplitude is the most common channel characteristic to generate the secret key. The received signal by Alice and Bob can be given by:

$$y_A = x(t)|h(t)| + n_A(t) \quad (1)$$

$$y_B = x(t)|h(t)| + n_B(t) \quad (2)$$

where $x(t)$ is the transmitted signal, $|h(t)|$ is the channel gain and $n_A(t)$ and $n_B(t)$ are the additive white Gaussian noise (AWGN) at Alice and Bob's receivers, respectively. Then the estimated channel gain $|\widehat{h}(t)|$ by Alice and Bob's receiver are:

$$|\widehat{h}_A(t)| = |h(t)| + z_A(t) \quad (3)$$

$$|\widehat{h}_B(t)| = |h(t)| + z_B(t) \quad (4)$$

Where $z_A(t)$ and $z_B(t)$ are noise in estimation of $|h(t)|$ at Alice and Bob, respectively. $|\widehat{h}_A(t)|$ and $|\widehat{h}_B(t)|$ are highly correlated. Since Eve listens to all the communication between Alice and Bob, the received signal at Eve's receiver for both signals can be given by:

$$y_E^A = x(t)|h_E^A(t)| + n_E(t) \quad (5)$$

$$y_E^B = x(t)|h_E^B(t)| + n_E(t) \quad (6)$$

where $|h_E^A(t)|$and $|h_E^B(t)|$ are the channel gains between Alice and Eve; and Bob and Eve, respectively. Since it is assumed that Eve can not be less than half wavelength near from either Alice or Bob, $|h_E^A(t)|$ and $|h_E^B(t)|$ are independent from $|\widehat{h}_A(t)|$ and $|\widehat{h}_B(t)|$.

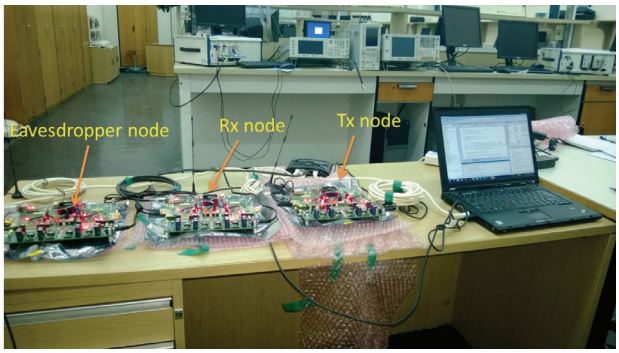

Fig. 1: Experimental Setup for the channel gain estimation

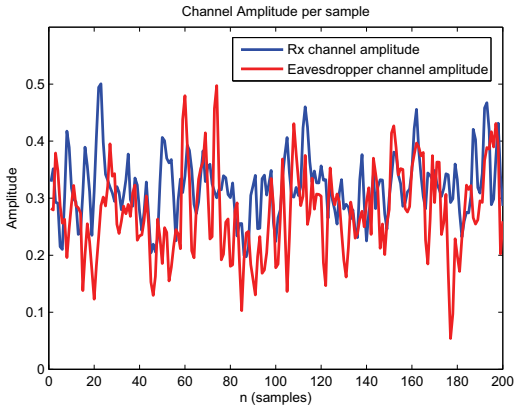

Fig. 2: Implementation of channel gain estimation: channel amplitude measurements.

The channel gain estimation is implemented on the WARP platform [22]. We use three WARP nodes in our scenario, one is set as the transmitter (Tx), Alice, the second as the intended receiver (Rx), Bob, and the third as the eavesdropper receiver, Eve. Each WARP node has two RF daughter cards operating as a transceiver in the WiFi band. Figure 1 shows our experimental setup after programming the FPGA on the three nodes. Without loss of generality, our test environment is an indoor non-line of sight environment. In other words, our algorithm can be implemented in any other environment whether its an indoor or outdoor, line of sight or non-line of sight. The Rx node and the eavesdropper node were placed on the corners of the lab while Tx node was at the back of the lab. The separation between the Rx and the eavesdropper was much larger than half the wavelength to avoid channel gain correlation. We estimated the channel gain for both the Alice-Bob channel as well as the the Alice-Eve channel. Figure (2) shows the channel amplitude for the two channels for 200 samples. One can see that even in an indoor lab environment the channel amplitude measurements between Alice and Bob are independent from the ones between Alice and Eve. In a strong line of sight environment, the channel gain measurements will be highly correlated.

IV. Distance Estimation Based On RSSI Measurements

Most of the currently deployed radios are equipped with RSSI estimation circuitry. If the Tx-Rx radio propagation model is known, RSSI can be used to estimate the distance between the two communicating nodes, Alice and Bob. Also distance estimation based on RSSI readings does not require additional hardware for time synchronization such as the TOA based algorithms. The RSSI readings measured by Eve can determine the distance between itself and between either Alice or Bob. Eve can only estimate the distance between Alice and Bob if Eve's radio is equipped with AOA estimation system. In this case, given the two angles between Eve and Alice, and Eve and Bob and the two distances, Eve can estimate the distance between Alice and Bob.

Unlike the free space propagation model and the two ray ground model, the log distance path loss model is a more general model that can be used for both indoor and outdoor environments. The log distance path loss model is given by:

$$\overline{P_r(d)}(dBm) = P_r(d_0)(dBm) - 10n_p \log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \tag{7}$$

where $\overline{P_r(d)}$ is the average received power in dBm, which is the RSS, $P_r(d_0)$ is the received power at a reference distance d_0, n_p is the path loss exponent and X_σ is a normally distributed random variable with zero mean and σ standard deviation. Using a reference distance of 1 meter the equation reduces to:

$$\overline{P_r(d)} = -10n_p \log_{10}(d) + C \tag{8}$$

where C is $P_r(1) + X_\sigma$. The distance can then be estimated as:

$$d = 10^{-\frac{RSS-C}{10n_p}} \tag{9}$$

For the non-line of sight indoor environment similar to our model, using linear regression estimation, [23] represents Eq. (8) as:

$$P_r(d) = -23.411 \log_{10}(d) - 48.676 \tag{10}$$

Based on the environment, Eq(10) changes. One has to collect empirical data and adjust Eq(10) accordingly to minimize the estimation error.

The RSSI readings obtained from our WARP nodes have a dynamic range of 0 to -92 dBm. The average RSSI reading for the received samples after conversion is -68.2 dBm for Bob and -72 dBm for Eve. The measured distance between Alice and Bob is 3.6 meters and between Alice and Eve is 7.5 meters. Based on our non-line of sight indoor environment and WARP kits reading, we adjust Eq.(10) to be:

$$P_r(d) = -20.114 \log_{10}(d) - 55.8 \tag{11}$$

The estimated distances between Alice and Bob and Alice and Eve are then 4.04 and 7.16 meters, respectively.

V. Secret Key Generation Based on Both Channel and Distance Measurements

Now that we have collected channel gain measurements and estimated the distances between the two communicating nodes based on RSSI measurements, we will use these two parameters as common sources of randomness. Even if the eavesdropper is equipped with AOA estimation capabilities, it will not be able to break the secret key since it exploits the channel between Alice and Bob. Or if the environment is a line of sight environment, that highly depends on the distance, and Eve can estimate the channel gain between Alice and Bob based on signal she receives from either of them, it still can not estimate the distance between them. The only vulnerability in our algorithm is when Eve's radio is equipped with AOA estimation capabilities and the environment is a strong line of sight with minimal multipath effect. In this case, Eve can estimate both the distance between Alice and Bob and the channel gain. In this case the bit operation applied at the two sources of randomness, through our algorithm, is still not known to Eve. We will show in the next section that even in the *worst case scenario*, the secret key generated based on our algorithm can not be recovered by Eve.

After collecting the measurements above our algorithm adapts the following steps to generate the secret key.

A. Quantization

Now that we have two common sources of randomness, the first step of our algorithm is to convert them into a bit stream suitable for the secret key generation. The conventional secret key length is between 128 and 512 bits [5]. We use the most popular technique for quantization which is the uniform quantization [24]:

$$Y = Q(X) \qquad X \in (d_i, d_{i+1}) \tag{12}$$

where d is the interval and X is the input, which in this case is our channel and distance measurements. In the uniform quantization, the spaces along the x-axis, i.e., time, is uniformly distributed. Similarly for the spaces in the y-axis, i.e., the channel amplitude for the first common source of randomness and the estimated distance for the second.

B. Encoding

Although uniform quantization is easy to implement, increasing the quantization bit number, dramatically degrades the performance of the algorithm since the bit mismatch rate between the two communicating nodes increases. In [4], an encoding algorithm is proposed to tackle this problem where each uniformly quantized value is encoded with multiple values.

C. Combining the Two Bit Streams

Now that we have measured, quantized and encoded our two common sources of randomness, we have two bit streams containing these data. To combine these two bit streams, any logical operation such as AND, OR or concatenation can be applied on the two bit streams to generate a single bit stream

containing both channel amplitude and distance information. We choose to use the XOR operation with the two bit streams as the inputs to generate the single bit stream. *It is worth noting that we chose a simple bit operation to be applied on the bit streams for the sake of simplification*. One can apply a more complicated operation at the bit streams such as bit masking or combinations of series and parallel logical gates. We will show that even with simple bit operation that is not known to the eavesdropper, our algorithm outperforms the two other algorithms.

D. Information Reconciliation

The generated bit streams at Alice and Bob will have some discrepancy. This is due to several reasons such as interference, noise and hardware limitations. Another reason is that channel fading can cause inaccuracy in the RSSI readings, and therefore, the measured distance at Alice and Bob will not be identical. We adopt the reconciliation protocol presented in [25] to minimize the discrepancy. Both Alice and Bob first permute their bit streams in the same way. Then they divide the permuted bit stream into small blocks. Alice then sends permutations and parities of each block to Bob. Bob then compares the received parity information with the ones he already processed. In case of a parity mismatch, Bob changes his bits in this block to match the received ones. This protocols leaks an amount of information to Eve close to the minimum.

E. Privacy Amplification

Although information reconciliation protocol leaks minimum information, Eve can still use this leaked information to guess the rest of the secret key. Privacy amplification solves this issue by reducing the length of the outputted bit stream. The generated bit stream is shorter in length but higher in entropy. To do so, both Alice and Bob apply a universal hash function selected randomly from a set of hash functions known by both Alice and Bob. Alice sends the number of the selected hash function to Bob so that Bob can use the same hash function. Our algorithm is summarized below.

Algorithm 1 Secret Key Generation algorithm

Step 0: Initialization
Alice and Bob exchange signals
Alice and Bob collect sequences of channel amplitude measurements
Alice and Bob collect sequences of RSSI
Alice and Bob use average RSSI to estimate distance
Step 1: Uniform Quantization
Alice and Bob quantize channel amplitude measurements using $Y = Q(X) \quad X \in (d_i, d_{i+1})$
Alice and Bob quantize estimated distance using $Y = Q(X) \quad X \in (d_i, d_{i+1})$
Step 2: Encoding
Alice and Bob encode each uniformly quantized value with multiple values
Step 3: Combining the Two Bit Streams
Alice and Bob apply bit operation on the two bit streams (e.g., XOR)
Step 4: Information Reconciliation
Alice and Bob permute the bit stream and divide them into small blocks
Alice sends the permutation and parities to Bob
Bob compares the received parity information with his
In case of mismatch, Bob corrects his bits accordingly
Step 5: Privacy Amplification
Alice sends the number of the hash function to Bob
Alice and Bob apply the hash function to the bit stream

VI. Performance Evaluation

Now that we have presented an implementation test-bed for our algorithm, we evaluate its performance through extensive iterations. We implement our algorithm for the *worst case scenario* where the eavesdropper, Eve (E), can estimate the distance between Alice (A) and Bob (B) and Alice , Bob and Eve are in a strong line of sight environment. We simulate our algorithm in a Rician fading channel with high K-factor. We apply a simple bit operation on the two bit streams, which is not known to Eve, for the sake of simplification. Alice and Bob apply XOR while Eve applies a different bit operation, which is AND. Again, we note that the bit operation applied at Alice and Bob can be more complicated by applying a combination of series and parallel logical gates, which Alice and Bob agreed on and not known to Eve.

We generate the secret key for our algorithm and compare it to the secret key generated by the channel-only and distance-only algorithms. We compare the bit mismatch rate (BMR) of the generated secret key between A-B and between A-E after quantization and encoding for the three algorithms; namely: channel only, distance only and our hybrid channel and distance (after combining the two bit streams step). We also compare the entropy of the secret key generated at either Alice or Bob to the entropy of the secret key generated at Eve for the three algorithms. In Table. I we summarize the simulation parameters for all the subsequent figures.

TABLE I: Simulation Parameter for all the Subsequent Figures

–	Fig. 3	Fig. 4	Fig. 5	Fig. 6
SNR A&B	10	15	10	10
SNR E	10	0:1:30	10	10
K-factor A-B	15	16	16	16
K-factor A-E	0:1:30	4	4	4
Channel Iter.	200	200	25:25:400	200
No. Iter.	10000	10000	10000	10000
A &B Dist. STD	0.92	0.92	0.92	2.25
E Dist. STD	1.73	1.73	1.73	0:12

In Fig. 3, we present the simulation results for the three algorithms when the A-B channel's K-factor remains constant at 15 and the K-factor for the A-E channel changes between $0:30$. The standard deviation of the estimated distance at Eve is higher than that for either Alice and Bob due to AOA error as well as the errors in estimating the distances based on the received RSSI's. The mean in the two cases is 10 meters. One can see that A-B BMR for our algorithm is close to the minimum achieved by the distance-only algorithm, which is less than the conventional acceptable rate of 0.15. At the same time, the A-E BMR is the highest for our algorithm ($\simeq 0.4$). The entropy of the secret key generated at either Alice or Bob for our algorithm is higher than the achieved entropy of the key generated by the two other algorithms. While the entropy of the secret key generated by Eve through our algorithm is the lowest. In other words, our algorithms is achieving a higher secrecy rate than the other two algorithms. The A-E BMR for the channel-only algorithm increases at lower values of K-factor,i.e., weaker line of sight environment and saturates as the K-factor increases. Correspondingly, the BMR of our algorithm is slightly lower at lower values of the K-factor.

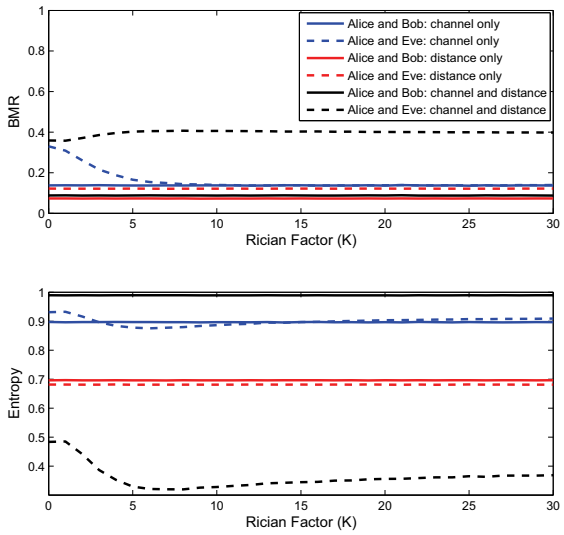

Fig. 3: Estimated BMR and entropy between Alice and Bob and Alice and Eve for channel only, distance only and both channel and distance algorithm with the Rician K factor changes at Eve's channel.

In Fig. 4, we present the simulation results for the three algorithms when the SNR of the received signal by either Alice and Bob remains constant at $10dB$ and the received SNR by Eve changes between $0:30$. Again, the A-B BMR for our algorithm is low, close to the minimum achieved by the distance-only algorithm and the highest between A-E. At the same time, the entropy of the secret key generated at either Alice or Bob for our algorithm is higher than the achieved entropy for key generated by the two other algorithms. At lower values of Eve's received SNR, the performance of the channel-only algorithm was highly degraded since the A-B BMR and the A-E BMR are very comparable. The performance of our algorithm was slightly affected by changing Eve's SNR.

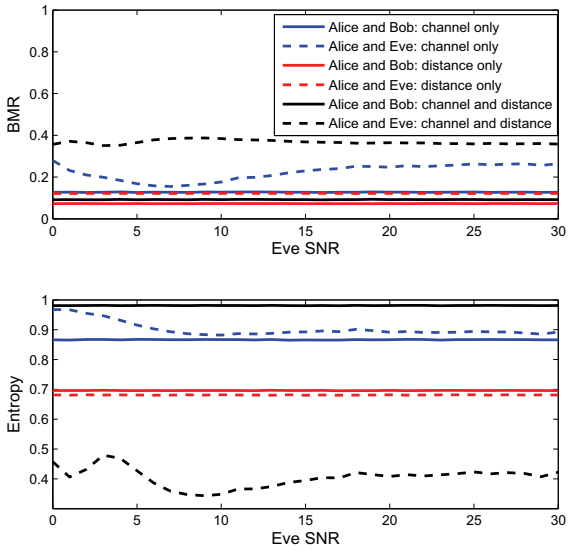

Fig. 4: Estimated BMR and entropy between Alice and Bob and Alice and Eve for channel only, distance only and both channel and distance algorithm with Eve's received SNR changes.

It's worth noting that changing either SNR or the Rician K-factor can be viewed as simulating the mobility of Eve. In other words, Eve is moving to improve its BMR with Alice or Bob.

In Fig. 5, we present the simulation results for the three algorithms when the number of channel amplitude measurement iterations changes from $25:400$. As the number of the collected channel amplitude measurements increases, the performance of the channel-only algorithm degrades. Although

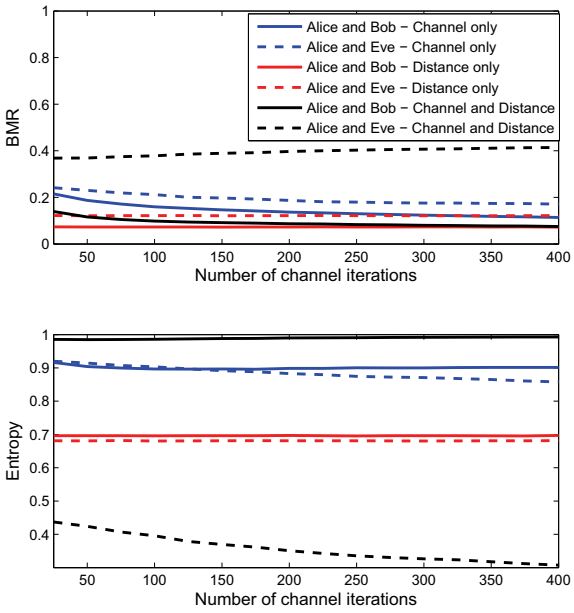

Fig. 5: Estimated BMR and entropy between Alice and Bob and Alice and Eve for channel only, distance only and both channel and distance algorithm when the number of collected channel iteration changes.

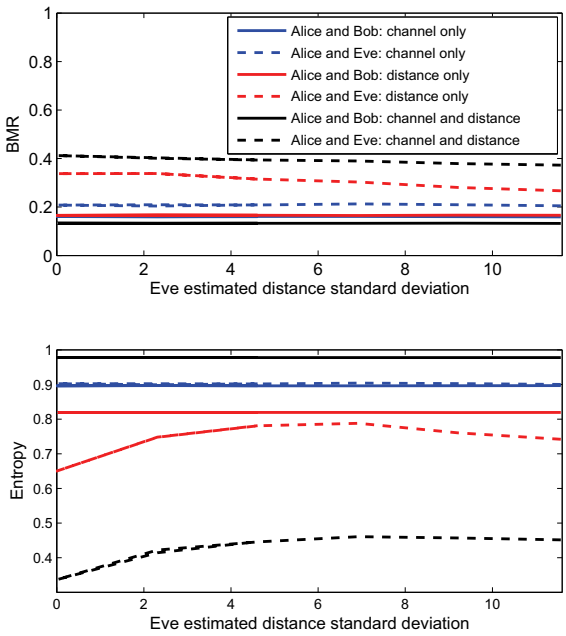

Fig. 6: Estimated BMR and entropy between Alice and Bob and Alice and Eve for channel only, distance only and both channel and distance algorithm when Eve's estimated distance standard deviation changes.

the entropy of the secret key generated by our algorithm was not affected, averaging a larger number of channel amplitude measurements highly reduces the entropy of the secret key generated by Eve which is another advantage for our algorithm. Sill our algorithm outperforms the two other algorithms through maintaining a low A-B BMR and the highest A-E BMR.

In Fig. 6, we present the simulation results for the three algorithms when the standard deviation (STD) of the estimated distance between Alice and Bob remains constant at 2.25 and standard deviation of the estimated distance by Eve changes between $0 : 12$. The mean in the two cases is 20 meters. One can see that performance of the distance only-algorithm was highly affected by changing the standard deviation of the estimated distance by Eve. Changing the standard deviation of the Eve's estimated distances simulates the errors of estimating the two RSSI's and the two AOA's. The performance of our algorithm was again slightly affected.

VII. Conclusion

In this paper we propose a novel secret key generation algorithm that is based on both the reciprocity of the channel as well as the distance between the two nodes trying to secure a communication link. Exploiting a second common source of randomness overcomes the vulnerability of using either of them. We modified an indoor path loss model to estimate the distance between the communicating nodes based on RSSI readings. Exploiting a second source of randomness does not add a significant complexity to the system since distance estimation is based on the RSSI reading and we apply a simply bit operation at the two bit streams generated. We then evaluated the performance of our algorithm through extensive iterations for the worst case scenario. We studied the performance of our algorithm when Eve' Rician K-factor, received SNR, estimated distance standard deviation and number of channel iterations are varied. We plotted the BMR and entropy of the secret key generated through our algorithm and compared it to the channel-only and distance-only algorithms. Our algorithm consistently outperformed the two other algorithms; achieving a low BMR between Alice and Bob and the highest BMR between Alice and Eve. At the same time the entropy of the secret key generated by either Alice or Bob was much higher than that achieved by Eve and higher than that achieved by the two other algorithms. Also, the entropy of the secret key generated by Eve through our algorithm was the lowest when compared with the entropy of the secrecy key generated by Eve through the two other algorithms. Hence, our algorithm is achieving a higher secrecy rate which is the advantage of exploiting a second common source of randomness.

Acknowledgment

This research was made possible by NPRP 5-559-2-227 grant from the Qatar National Research Fund (a member of

The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] G. Smith, "A direct derivation of a single-antenna reciprocity relation for the time domain," *Antennas and Propagation, IEEE Transactions on*, vol. 52, no. 6, pp. 1568–1577, 2004.

[2] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 401–410. [Online]. Available: http://doi.acm.org/10.1145/1315245.1315295

[3] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM Workshop on Wireless Security*, ser. WiSe '06. New York, NY, USA: ACM, 2006, pp. 33–42. [Online]. Available: http://doi.acm.org/10.1145/1161289.1161297

[4] J. Zhang, S. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1–5.

[5] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 128–139. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409960

[6] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 240–254, 2010.

[7] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 3, pp. 364–375, 2007.

[8] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 17–30, 2010.

[9] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *Mobile Computing, IEEE Transactions on*, vol. 12, no. 5, pp. 917–930, 2013.

[10] O. Gungor, F. Chen, and C. Koksal, "Secret key generation from mobility," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, 2011, pp. 874–878.

[11] O. Güngör, F. Chen, and C. E. Koksal, "Secret key generation from mobility," *CoRR*, vol. abs/1112.2793, 2011. [Online]. Available: http://arxiv.org/abs/1112.2793

[12] U. Maurer, "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on*, vol. 39, no. 3, pp. 733–742, 1993.

[13] Y. Shen and M. Win, "Fundamental limits of wideband localization x2014; part i: A general framework," *Information Theory, IEEE Transactions on*, vol. 56, no. 10, pp. 4956–4980, 2010.

[14] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch, H. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *Signal Processing Magazine, IEEE*, vol. 22, no. 4, pp. 70–84, 2005.

[15] Z. Zhang, C. Law, and Y. Guan, "Ba-poc-based ranging method with multipath mitigation," *Antennas and Wireless Propagation Letters, IEEE*, vol. 4, no. 1, pp. 492–495, 2005.

[16] J.-Y. Lee and R. Scholtz, "Ranging in a dense multipath environment using an uwb radio link," *Selected Areas in Communications, IEEE Journal on*, vol. 20, no. 9, pp. 1677–1683, 2002.

[17] L. Mailaender, "On the geolocation bounds for round-trip time-of-arrival and all non-line-of-sight channels," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, p. 584670, 2008. [Online]. Available: http://asp.eurasipjournals.com/content/2008/1/584670

[18] Y. Qi, H. Kobayashi, and H. Suda, "Analysis of wireless geolocation in a non-line-of-sight environment," *Wireless Communications, IEEE Transactions on*, vol. 5, no. 3, pp. 672–681, 2006.

[19] D. Niculescu and B. Nath, "Ad hoc positioning system (aps) using aoa," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3, 2003, pp. 1734–1743 vol.3.

[20] A. Molisch, *Wireless Communications*. Wiley-IEEE Press, 2005.

[21] N. Patwari and A. O. Hero, III, "Using proximity and quantized rss for sensor localization in wireless networks," in *Proceedings of the 2Nd ACM International Conference on Wireless Sensor Networks and Applications*, ser. WSNA '03. New York, NY, USA: ACM, 2003, pp. 20–29. [Online]. Available: http://doi.acm.org/10.1145/941350.941354

[22] "Warp project." [Online]. Available: http://warpproject.org

[23] R. Al Alawi, "Rssi based location estimation in wireless sensors networks," in *Networks (ICON), 2011 17th IEEE International Conference on*, 2011, pp. 118–122.

[24] L. Tan, *Digital Signal Processing Fundamentals and Applications*. Academic Press, 2007.

[25] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion." Springer-Verlag, 1994, pp. 410–423.