JOURNAL FOR INNOVATIVE DEVELOPMENT IN PHARMACEUTICAL AND TECHNICAL SCIENCE

Volume-2,Issue-4 (Apr-2019)
ISSN (O) :- 2581-6934

Secret Group-Key Generation with Symmetrically Quantized GSK at physical Layer for Multi Antenna Mesh Topology

C.M.Supriya[1], Ms.S.Afrin Banu [2]
[1]Student ME , [2]Assistant Professor ME
[1 2] Computer Science and Technology, Rajas Institute of technology for women.

Abstract— A secret group key generation scheme in physical layout has been proposed in this paper where a mesh topology along with a multi-antenna passive eavesdropper consists the existence of an arbitrary number of multi-antenna LNs. In the scheme's first phase, the transmission of pilot signals from selected antennas of every node takes place where a channel is linked to each node. By the use of selected coefficient, every node linearly broadcasts an estimated combination of the selected channel information. This is the second phase. The data of the channel which is used for group key generation can be obtained by other LNs where the eavesdropper cannot do it. The generation of group by each node includes the sequential steps of quantization and encoding the estimated channels into keys. Common quantization schemes like scalar and vector quantization are applied and their performance is compared. For further enhancement of key generation performance, the aspects to determine the antennas of each node that we use for group key generation are provided. With the help of several key-related measurements, the simulation results evaluate the efficiency of the proposed group key generation scheme. A test bed is also implemented with the help of universal software radio peripheral in order to determine practical durability of our scheme. The generated key that passes the above test bed and also the national institute of standards and technology test suit is eligible for secrecy of elimination.

1. INTRODUCTION

In wireless communication, physical layer key generation has been studied a lot as there is no requirement for any network infrastructures and it also has compatibility with eavesdropper having unlimited computing capacity. Key generation between two legitimate users has been mostly focused concerning physical layer secret key generation. But in certain cases sharing confidential information only among people in a group necessarily needs a common-key to be generated for the members of the group. For example, the secret information about a crime is shared between police is by a secret group key.

This makes easy for the two users to get channel information. In order to share that particular information with more users it has to be forwarded by the two users first. This system has a risk of information leakage to eavesdroppers. The next challenging part is when there are more users, more number of channels are included in the process that can be made use of to create a part of Key. Considering large and more channels long group key can be created. With channels being the same, a scheme needs long channel coherence time, since it takes more time to send all information of those channels. With more options for the arrangement of transmission and selection of parameter, optimization of the parameters becomes more challenging.

Concerning different topologies and researching various channel information, schemes for secret group key generation or proposed. Methods of generating a secret key for a certain amount of nodes are written with the use of information theoretic methods. But these types of proposals only concern about communications which are noiseless between the nodes that are not certain to work practically. The reference channels are selected from the side and the Centre node and firstly determined. The Centre node sends the output of RSS's difference of the reference channel and the channel that is linked to side node two other side node. At last every node could have information of reference channel and group key is generated using them.

Mesh topology is not meant for generation of group key since it has to be created newly to gain higher performance in generating group key.

With the help of information that is gained from impulse radio ultra-wideband multipath channels, a 3 node mesh topology having a public common channel is used to create a group key. But there is no analyzation of attack by eavesdroppers and leaking of information by the process of reducing from bulk broadcast messages. Also there is no number of group users. There is a proposed algorithm for secret key that can be used in group but that's only for single antenna nodes. Considering a couple of channels transmission of bit string can be achieved by XOR ing two bit strings. XOR ing is combining fixed coefficient which is less efficient than that of optimized coefficients.

The secret key rate and key disagreement property is mainly based on the quantization scheme selection. Concerning the system of quantization in secret key generation, it was advised to get the output of the multiplication of optical matrix and estimated channels before the process of quantization which is mainly proposed to eliminate the estimated channel out of the quantization boundaries. Quantization scheme has also been optimized to reduce quadratic distortion and KDP. Another method was created to regular interval guard of quantization. But these schemes can only be used to generate key among two users and can be used for a group of people hence there is no sense using this scheme where several users are involved.

A Novel secret group key generation scheme has been proposed in the paper concerning mesh topology where more number of antennas are equipped in every node and other nodes are interlinked through direct channels. As every node has the ability to hear the pilot signal from any area in mesh topology, we prefer using information from multiple channels to information from one channel in order to maximize key rate.

As an important note there are two types of pace in this scheme. The first one is sounding phase where every node transmits pilot signals. The second one is broadcast phase. Here broadcast of weighed combo of various estimated channels with regulated coefficients by every node takes place. Considering broadcast phase, information can be broadcasted several times by nodes for the reception of needed signal dimensions for the estimation of required channels.

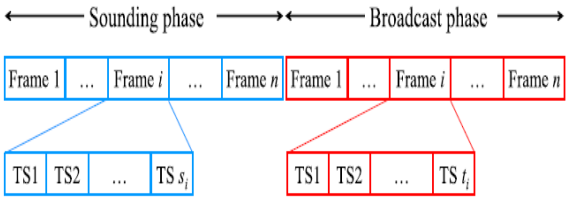
To make virtual transmission rank to a receiver necessarily larger for estimation of needed channels, different coefficient sets should be selected for different time slots.

II. PROPOSED GROUP-KEY GENERATION SCHEME

In this section, we first briefly describe the secret group-key generation scheme with general variables. Second, we presentthe transmission, estimation, and quantization of the schemein details.

A. Brief Description of the Scheme

First, we select the channels used for the key generationsince the channel coherence time may be



not long enough to finish pilot transmissions for all available channels. Hence, we select$l_{j,i}$ antennas of A_i to connect to $A_j$and select $l_{i,j}$antennas ofA_j to connect to Ai where $1 \leq l_{j,i} \leq m_A, \forall i \neq j$. The number of selected channels between A_i and $A_j$is thus$l_{j,i} l_{i,j}$.

The scheme is divided into two phases called the sounding phase and the broadcast phase. Each phase is then divided into n frames. Denote the set of all selected channels to be used in the proposed scheme and the number of those channels $q \triangleq |Q|$.

The i-th frame of the sounding phase is divided into s_i time slotswhere$s_i \triangleq \max_j l_{j,i}$.In time slot α of frame i, antenna α of A_i transmits a pilot signal so that all other LNs can estimate the channels between antenna α of $A_i$and the selected antennas of those nodes. After this sounding phase, Ai can estimate$q_i^1 \triangleq \sum_{i=1}^{n} l_{j,i} l_{i,j}$ channels linked to it.

Superscript 1 refers to the first phase. We denote the set of these channels as Q^1_i, and $Q^1_i \subset Q$. The i -th frame in the broadcast phase is divided into $t_i$time slots. In each time slot, $A_i$broadcasts the information of the channels it estimated in

ISSN:-2581-6934|www.jidps.com

the sounding phase so that other LNs can estimate the channels that they did not estimate in the sounding phase.

B. Key Generation

We now present the transmission, estimation, and quantization processes of the two phases in more details. In this description, for the sake of simplicity, we assume that the number of selected antennas from a LN connected to other LNs are the same, i.e.,$l_{i,j} = 1, \forall i \neq j$.We also assume that the numbers of antennas and the numbers of time slots, used by each LNs, are equal, i.e., $f_i = l$, and$t_i = t_{O,} \forall i$

Algorithm 1 Group-Key Generation Algorithm at a LN

Data: m_A, m_E, $\delta^2_{i,j}$, $\delta^2_{i,E}$, n, ζ, i, T.

Result: The secret group key.

Steps:

- Compute $l = \lfloor \frac{T}{n} \rfloor, f_i = \lfloor \frac{T}{n} \rfloor$, $t_i = \lfloor \frac{T}{2n}(n-2) \rfloor$ for $i \leq \kappa_o$ and $t_i = \lceil \frac{T}{2n}(n-2) \rceil$ for $i > \kappa_o$, κ_o is given in (49).
- Transmit a pilot signal from antennas 1 to l in frame i.
- Receive pilot signals in the other frames of the sounding phase, estimate by $\hat{\mathbf{g}}_i^1 = \xi_i \mathbf{y}_i^1$.
- Use (55) to compute $\mathbf{R}_i^k$.
- Transmit the combinations accordingly.
- Use (7) to estimate the other channels.
- Quantize and encode all estimated channels to binary strings, and concatenate them to a single key.

There are l^2 channels between any two nodes which are used for key generation. There are$\frac{1}{2}\, n(n-1)$ links among n nodes, hence, q =$\frac{1}{2}\, n(n-1)l^2$. On the other hand, in the sounding phase, a node received pilot signal from n − 1 other nodes, thus, $|Q^1_i|$ = (n − 1) $l^2 \triangleq$ q1.In the broadcast phase, a node needs to estimate the channels in Q which have not been estimated, hence,

$|Q_i^2| = \text{q} - \text{q1} = \frac{1}{2}(n-1)(n-2)l^2 \triangleq q2, \forall i \in \{1, \dots, n\}$.

1) Sounding and Broadcast Phases: In this section, we describe the pilot transmissions, channel estimations, and the broadcasting of the channel combinations. In the n − 1 frames of the sounding phase, A_i receives $(n-1)l$signals which can be written in a vector given by$y_i^1 = g_i^1 + v_i$ where $v_i \in \mathbb{C}^{(n-1)l \times 1}$ is complex Gaussian noise. A_i estimates $g^1{}_i$ by

$$\boldsymbol{g_i^1 = \xi_i y_i^1}$$

Where $\xi_i = 1$ for ZF and $\xi_i = \frac{1}{1+\sigma^2}$ for MMSE.

2) Quantization: After all necessary channels are estimated at the LNs, they are quantized and encoded into bit streams. The bit streams are then concatenated into the final secret keys. Each channel considered in this paper depends on two independent random variables, real and imaginary parts. We refer them as two information dimensions of our scheme. Two information dimensions can also be magnitude and phase when the estimated channels are seen in the polar coordinates. In some works, only one information dimension such as the magnitude of an estimated channel, represented by the signal strength, is used. This is because it is generally easier to be measured in practice than the phase. However, phase has also been used for key generation. In fact, our proposed scheme can work with both cases, one and two information dimensions per channel. How they are quantized, encoded and concatenated depends on the number of secret keys $n_K$we want to generate in the scheme. They also depend on the quantization method we use.If the number of keys is one, i.e., $n_K = 1$, each node combines all the information of q channels into one key by one of the following two methods:

- **Scalar quantization (SQ):** We independently quantizes each information dimension. We choose the quantization steps to guarantee that the probabilities that a variable corresponding to the information dimension falls into each quantization intervals are equal. This maximizes the key entropy. If the variable corresponding to that information dimension is a real or imaginary part of a channel, which is normally distributed, we can choose the quantization intervals.

Vector quantization (VQ): This method gives a lower KDP, but it is much more complicated than SQ. One efficient algorithm of VQ is Linde-Buzo-Gray (LBG). After the estimation of q channels, we have 2q information dimensions for real and imaginary parts of the estimates. We divide 2q information dimensions inton_V groups, each of which corresponds to a vector and has $n_D \triangleq {}^{2q}/_{n_V}$information dimensions.

Each $n_D$dimensional vector can be quantized to $n_D n_B$ bits. Concatenating all n_V groups leads to $n_V n_D n_B$ = $2qn_B$ bits in the final key. Figure (b) shows the processing steps of VQ with n_D = 4 and n_V = 1. Note that VQ does not shorten the key when it merges several information dimensions into a quantization. If the number of quantization is reduced by a factor, the number of bits in the output in a quantization increases by the same factor.

ISSN:-2581-6934|www.jidps.com

C. Minimizing Information Leakage

In this section, we propose the method to limit the information of the key exposed to the eavesdropper. We denote $g_E^1 = \left[h_{1,E}^{1,1}, h_{1,E}^{1,2}, \dots, h_{1,E}^{1,1}, h_{2,E}^{1,1}, \dots, h_{n,E}^{1,1}\right]^T$ as the vector consisting of channels linked to E, while $g_E^2 = \left[h_{1,2}^{1,1}, h_{1,2}^{1,2}, \dots, h_{1,2}^{1,1}, h_{1,2}^{1,2}, \dots, h_{1,2}^{1,1}, h_{1,3}^{1,1}, \dots, h_{n,n}^{1,1}\right]^T$ is the vector consisting of the channels among the LNs, which are not linked to E, and used to generate the group key. After each LN transmits a pilot signal using its selected antennas, E receives the signals and tries to estimate each channel in g_E^1.

In the broadcast phase, each of n LNs broadcasts signals during t_o time slots using l antennas. By receiving those signals with m_E antennas at E, the number of signal dimensions E can distinguish is $nt_O \min(l, m_E) = nt_O l$dimensions, because$m_A \le m_E$, as assumed, and $l \le m_A$, while the number of channels E needs to estimate is $q_E^2 \triangleq |g_E^2| = \frac{1}{2}n(n-1)l^2$. The smaller t_O, the more unreliable the estimation at E. Hence, the maximum t_O satisfies

$$nt_O l < \frac{1}{2}n(n-1)l^2 \Leftrightarrow t_O < \frac{1}{2}(n-l)l$$

D. Secret Group Key Rate

In this section, we derive the secret group key rate (SGKR). Note that calculating the SGKR for an arbitrary n and noisy channels in both phases can lead to cumbersome expressions and require unnecessarily tedious steps. Hence, for analytical tractability, we derive the SGKR for the case of n = 3, single antenna, noiseless sounding phase, and noisy broadcast phase. We will introduce new notations only for this section to avoid the confusion to the ones in other sections.

III. IMPROVED DESIGN OF THE KEY GENERATION SCHEME

The proposed scheme in this paper is designed for a general case with given values of important system parameters such as the number of LNs n, the number of selected antennas in each node $l_{i.j}$, the number of time slots t_i each node broadcasts, and the combination coefficients R_j^ka node uses to broadcast in each time slot. Optimizing those parameters can enhance the key-generation performance of the proposed scheme. However, it is a hard problem since the performance metrics related to the key generation, e.g., secret group key rate (SGKR), KDP, key leaking probability (KLP), bit mismatch probability (BMP), and bit leaking probability (BLP), are complex and in intractable forms. To handle this problem, we introduce the normalized number of secure channel (NNSC), defined by

$$\gamma = \frac{q - qL}{tS}$$

Where q is the number of estimated channels to generate the key, qL is the number of overheard signal dimensions at the eavesdropper which bears the information about the estimated channels and tS is the number of time slots in the scheme. The NNSC in (30) determines the secret key generation rate, especially when we do not consider the channel estimation error and assume once any information of a certain LN is received at E, the corresponding estimated channel is not secure anymore. With those assumptions and by assuming that each estimated channel is quantized and encoded into an output stream with nB bits, the key rate achieved by LNs is given by $r = \frac{qn_B}{tS}$bits/channel use, while the leaked key rate by eavesdropper is given by $rL = \frac{q_L n_B}{tS}$bits/channel use. Then, the secret key generation rate, normalized by nB bits is presented as the NNSC.Using the NNSC, in this section, we handle the optimization problem using the following two sub-problems, and consequently, the combined solution of them is suboptimal: 1) maximizing the normalized number of secure channels (NNSCs) by designing the number of selected antennas and the number of time slots that each node uses in the transmission steps; and 2) minimizing the channel estimation errors at LNs and maximizing the errors at eavesdropper by designing the combination coefficient vector R_j^k, used in the broadcast phase. The larger number of channels used for key generation (q) in certain amount of time gives higher SGKR. Furthermore, the smaller number of combinations overheard by the eavesdropper (qL) gives lower SGKR. Therefore, increasing NSSC, which is optimized in a sub-problem of the SGKR optimization one, improves the SGKR. Although we do not mathematically prove this, it will be verified by simulation results in Section V.

ISSN:-2581-6934|www.jidps.com

A. Maximizing the Normalized Number of Secure Channels

The key generation scheme design based on the NNSC issue when we do not know the estimation performance at Eand LNs. In the following, we present the general problem ofmaximizing NNSC and solve the problem for a special case to provide a closed-form solution.

1) The General Case: We need to select the channels used to generate the secret key by considering the channel coherence time T since it may be not long enough to accommodate the sounding phase. To do this, we select the number of antennas at each LN li, j which is limited as

$$\mathbf{0} \leq \boldsymbol{l_{j,i}} \leq \boldsymbol{m_A} \textit{ for } \mathbf{1} \leq \boldsymbol{i,j} \leq \boldsymbol{n}$$

Note that certainly$l_{i,i} = 0, \forall i \in \{1 \dots, n\}$. The total number of used channels in the scheme is

$q = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} l_{i,j}\, l_{j,i} = \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} l_{i,j}\, l_{j,i}$Since A_i has different numbers of selected antennas linked to different nodes, i.e., $l_{j,i}$, it will transmit $\max_j l_{j,i}$ pilot signals from $\max_j l_{j,i}$ antennas. Since each pilot signal occupies one-time slot and all pilot signals from n nodes need to be transmitted in T, we obtain the following constraint

$$\sum_{i=1}^{n} \max_{j} \boldsymbol{l_{j,i}} \leq \boldsymbol{T} \textit{ for } \mathbf{1} \leq \boldsymbol{i} \leq \boldsymbol{n}$$

B. Sub-optimal Design of Coefficient Matrices in Broadcast Phase

As mentioned at the beginning of Section IV, in this section, we design the coefficient matrices R_j^k to reduce the channel estimation errors at LNs, which will finally reduce the KDP. In the k- th time slot of the j -th frame of the broadcast phase, A_j combines the estimated channels by multiplying them with matrix R_j^k as presented in (2). As a LN broadcasts over several time slots of its frame, it has to use different combination coefficients in different time slots. If the same combination coefficients are used in different time slots, the signals from A_j received at A_i over several time slots are the same, and the rank of Di is not large enough for Ai to estimate g_i^2. It is therefore necessary to design suitable R_j^k such that not only rank (D_i) ≥ q2 but also ΦA is small enough and ΦE is large enough.

The optimization is given by

$$\max_{R_j^k} \Phi_E(R_j^k)$$

s.t.$\phi_A(R_j^k) \leq \phi_0$

$$E\left[Tr\left(X_j^k(R_j^k)\left(X_j^k(R_j^k)\right)^H\right)\right] \leq p$$

IV. EXPERIMENT MEASUREMENTS

In this section, we provide performance of the proposed scheme using a test bed with software-defined radios (SDRs) to verify the practical robustness and efficacy of the scheme. For the test bed, we use Universal Software Radio Peripheral (USRP) 2952 series of National Instruments [26], and three USRPs represent three LNs, i.e. Alice, Bob, and Carol. The nodes transmit pilot's signals, estimate the channels, and generate the shared secret keys according to the proposed protocol. Information reconciliation and privacy amplification are employed to process the keys and ensure that all nodes agree on same key with sufficient randomness. The NIST test suite is used to evaluate the performance of the generated group key.

A. Experiment Setup: We conduct the experiment in our laboratory with dimension of 15m×20m using USRP-RIO 2952. The USRPs are programmed using Lab view Communication Design Suite (LCDS) and controlled by the central processor NI PXIe-8135. Each USRP is connected to NI PXIe 1082 chassis at a high speed of 800 MB/s via PCI Express x4 cables. It has 2 full-duplex transmit and receive channels with 40 MHz/channel of real-time bandwidth and a large DSP-oriented Kintex 7 FPGA.

The analog RF front end interfaces with the large Kintex 7 410T FPGA through dual ADCs and DACs clocked at 120MS/s. Each RF channel includes a switch allowing for time division duplex (TDD) operation on a single antenna using the TX1/RX1 port. This functionality was widely exploited in our experiment. The LCDS allows to split the code between host processor and

FPGA so that intensive and latency stringent calculations are done on FPGA while processor handles controls and data fetching. All experiments are conducted in indoor environment and at 2.484 GHz frequency band, finalized after

ISSN:-2581-6934|www.jidps.com

spectrum sensing, to avoid any interference to existing WiFi links.

B. Measurement Design and Keys Extraction

In accordance with the proposed scheme in the paper, we design and conduct required steps for the randomness extraction i.e., shared key generation which are detailed as follows:

1) Channel Estimation: We implement half-duplex TDD for the group of Alice, Bob and Carrol such that each node sends a training sequence so that other two nodes can measure channel between itself and the transmitter. After three turns, Alice-Bob and Alice-Carrol channels are known at Alice; Bob-Carrol and Bob-Alice channels are known at Bob; and Carrol-Alice and Carrol-Bob channels are known at Carrol. To guarantee mutual channel reciprocity, the group members are required to estimate these 6 channels within the coherence time, i.e., 25-30 ms for indoor environment at around 2.484 GHz. Hence, the channel estimation step was designed to switch from transmission mode to the receiving mode and back fast enough so that the three nodes can observe these channels within a slotted time. We tackle this by using the dedicated registers and digital frequency switching. There is a set of registers, known as Automatic Transmit/Receive (ATR) registers, on SDR daughterboard that can be used for accessing transceiver configuration, controlling daughter-board's power, mixer and antenna configuration. We incorporate out-of-band digital-frequency shift of Rx while the antenna port is in transmission mode to avoid leakage from the TX power amplifier which might couple in to RX and hence affects its sensitivity. Digital frequency does not need local oscillator retuning or any RF command and can be done on the FPGA instantaneously. After 2 more turns, 5 in total for this setup, each of the nodes has 3 channels. The outputs resulted from those 3 channels are then concatenated to form a long secret key leveraging the number of participants in group topology. The final sequence can be represented by $R_a \| R_b \| R_c$, R_a is channel strength between Alice and Bob and so on. Note that the group key leakage rate to the eavesdropper was not measured in the implementation. Errors in any of the channel observations at Eve will further amplify the error in the final sequence since subtraction will yield higher error variance.

Quantization: To generate secret keys from these noisy estimates, we use two-level adaptive quantizer with lower threshold q_i^- and upper threshold q_i^+ , given by$q_i^+ = \mu R_i + \alpha\sigma R_i \; and \; q_i^- = \mu R_i - \alpha\sigma R_i$, for I = {a,b,c}, where$\mu x \; and \; \sigma x$are the mean and variance of samples in a sequence X, respectively, and α is a tuning factor. At each node samples with amplitude between $q_i^+ \; and \; q_i^-$ are dropped, while elements with values above and below are assigned by 1 and 0, respectively. The mismatch rate, which is regarded as KDP, decreases with the tuning factor, α, for both a group of user and a pair of users. Moreover, the key lengths for those cases also decrease with α. On the other side, if the α is too low, the key length is high at cost of increased KDP. Consequently, we choose α in the range of [0.4, 0.5], and in this range, 240 bits were extracted as final group key from 400 channel samples (133 per node to be precise).

3) Information Reconciliation and Amplification: In practice, the channel reciprocity can be disturbed due to dissimilarities in hardware/antenna, half-duplex pilot transmission andRF disturbances. The disturbed reciprocity leads to quantization errors as well as the key mismatch. Therefore, the bit mismatches in the key need to be corrected through the reconciliation process. For the reconciliation, we use permute-and-bisect–based approach called Cascade. The bisect compares block parties to detect errors. The parities are equal and unequal based on even and odd number of errors, respectively. It uses iterative division of block into sub-blocks. In order to remove biases towards error distribution, random permutation is performed before the next bisection. Multiple rounds of permute-and-bisect are performed until the errors are nullified. Carrol listens to these packets and uses parity to correct its mismatched bits when possible. Then one of these again reconciles with Carrol using the same method and all necessary flips are done by Carrol only.

For the privacy amplification, which is used to cope with the information leakage to the adversary, we use hash lemma functions. At the end, we have secret group key of length of 256 bits, which is the same at Alice, Bob and Carrol. Note that Cascade demands numerous communications, so it

ISSN:-2581-6934|www.jidps.com

may be not suitable for topologies involving time-critical elements.For this case, light and fast reconciliation approaches like fuzzy-extractors can also be used.

4) Randomness Test: Before using in practical setup, we need to insure that keys are substantially random since an adversary can hack low-entropy secret keys. We use the NIST test suit [23] to verify the randomness of the keys generated from our implementation. We randomly choose 256-bit sequences achieved in multiple cases and topology configurations,

i.e., distance and orientation of nodes. We compute their p values for recommended tests. From the obtained test results in Table II, we can see that the group key generated using the proposed protocol is suitable for practical use since p is much greater than 0.01, which implies 99% randomness.

V. CONCLUSION

In this paper, we have proposed a novel scheme to generate secret group key for a general number of multi-antenna LNs in the presence of a multi-antenna eavesdropper. The scheme consists of a sounding phase, a broadcast phase, channel estimation, and quantization. We have also provided the improved design for the proposed scheme including 1) the best selection of the number of antennas and time slots used in the scheme to improve the secret group key rate and 2) the sub-optimal combination coefficient matrices in the broadcast phase to reduce the KDP while maximizing the KLP. Through the simulation results, we have shown that the group-key generation with a multi–antenna eavesdropper is feasible with a good performance, which is even enhanced by using the obtained system parameters in the improved design. Furthermore, using the testbed with software-defined radios (i.e., USRPs), we implement our proposed scheme for three-node case. We finally show that the generated group key in the testbed passes the NIST test, which shows the feasibility and the pratical robustness of our proposed scheme for communication security.

REFERENCES

[1] K. Ren, H. Su, and Q. Wang, “Secret key generation exploiting channelcharacteristics in wireless communications,” IEEE Wireless Commun., vol. 18, no. 4, pp. 6–12, Aug. 2011.

[2] T.-H. Chou, S. C. Draper, and A. M. Sayeed, “Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage,”IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1751–1764, Sep. 2013.

[3] T. Shimizu, H. Iwai, and H. Sasaoka, “Physical-layer secret key agreement in two-way wireless relaying systems,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 650–660, Sep. 2011.

[4] C. D. T. Thai, J. Lee, and T. Q. S. Quek, “Secret group key generation in physical layer for mesh topology,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2015, pp. 1–6.

[5] C. Thai, J. Lee, and T. Q. S. Quek, “Physical-layer secret key genera-tion with colluding untrusted relays,” IEEE Trans. Wireless Commun.,vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[6] L. Lai, Y. Liang, and W. Du, “Cooperative key generation in wireless networks,” IEEE J. Sel. Areas Commun., vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[7] Q. Wang, K. Xu, and K. Ren, “Cooperative secret key generation from phase estimation in narrowband fading channels,” IEEE J. Sel. AreasCommun., vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[8] Y. Liu, S. C. Draper, and A. M. Sayeed, “Exploiting channel diversity in secret key generation from multipath fading randomness,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[9] M. Wilhelm, I. Martinovic, and J. B. Schmitt, “Secure key generationin sensor networks based on frequency-selective channels,” IEEE J. Sel.Areas Commun., vol. 31, no. 9, pp. 1779–1790, Sep. 2013.

[10] S. Watanabe and Y. Oohama, “Secret key agreement from vector Gaussian sources by rate limited public communication,” IEEE Trans.Inf. Forensics Security, vol. 6, no. 3, pp. 541–550, Sep. 2011.

[11] I. Csiszár and P. Narayan, “Secrecy capacities for multiple terminals, “IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[12] A. Gohari and V. Anantharam, “Information-theoretic key agreement ofmultiple terminals—Part I,” IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

Libraries (ADL'98), 1998.