ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

The Private Key Capacity of a Cooperative Pairwise-Independent Network (PIN)

S.Gopalakrishnan[1], D.Suganya[2], S.Vennila[3]

Assistant Professor, Dept. Computer Applications, Pioneer College of Arts and Science, Coimbatore, India[1]

Student, Dept. Computer Applications, Pioneer College of Arts and Science, Coimbatore, India[2,3]

Abstract: This paper studies the private key generation of a cooperative pairwise-independent network (PIN) with M + 2 terminals (Alice, Bob and M relays), M ≥ 2. In this PIN, the correlated sources observed by every pair of terminals are independent of those sources observed by any other pair of terminal. In the PIN, the pairwise source observed by every pair of terminals is independent of those sources observed by any other pairs. Secrecy is required from an eavesdropper that has access to the public inter-terminal communication. All the terminals can communicate with each other over a public channel which is also observed by Eve noiselessly. the PK needs to be protected not only from Eve but also from the two relays. The objective is to generate a private key between Alice and Bob under the help of the M relays; such a private key needs to be protected not only from Eve but also from individual relays simultaneously. The private key capacity of this PIN model is established, whose lower bound is obtained by proposing a novel random binning (RB) based key generation algorithm, and the upper bound is obtained based on the construction of M enhanced source models. PK generation algorithms are extended to a cooperative wireless network, where the correlated source observations are obtained from estimating wireless channels during a training phase. The two bounds are shown to be exactly the same. Then, we consider a cooperative wireless network and use the estimates of fading channels to generate private keys. It has been shown that the proposed RB-based algorithm can achieve a multiplexing gain M − 1, an improvement in comparison with the existing XOR- based algorithm whose achievable multiplexing gain is ⌊M⌋/2.

Keywords: PIN model, Private key capacity, Multiplexing gain, co-operative PIN model, index security.

I. INTRODUCTION

The pairwise-independent network (PIN) was introduced in [1] for secret key generation. Since then, many other related works have also investigated a variety of PIN models (e.g., [2]– [4]), and each of them aimed to find the secret key capacity of a particular PIN model. The PIN model is actually a special case of the multi-terminal "source model" [5], [6], in which the correlated sources observed by every pair of terminals are independent of those sources observed by any other pair of terminal. Note that the so-call "source model" was first studied by Ahlswede and Csisa´r for generating secret keys between two terminals using their correlative observations and public transmissions [7]. In recent years, the PIN model has been applied to practical wireless communication networks for key generation. Based on channel reciprocity, the correlated source observations in a PIN model can be obtained via estimating the wireless fading channels associated with legitimate terminals. This is because all the wireless channels in a network are mutually independent as long as the terminals are half-wavelength away from each other [8]. This physical layer (PHY) security approach has been recognized as a promising solution for generating secret key in recent years (e.g., [9]–[12]). Existing works have demonstrated that user cooperation can effectively enlarge the key capacity by introducing additional helper nodes for cooperative key generation [5], [11], [12]. The work in [5] first studied cooperative key generation (including the generation of secret keys and private keys) in a single-helper discrete memoryless source (DMS) model, where the private key needs to be protected not only from the eavesdropper but also from all the helper node. The works in [11], [12] utilized estimates of wireless channels for the key generation in cooperative wireless networks, in which the relay nodes provide additional resources of wireless fading channels. In [11], a relay-assisted algorithm was proposed to enhance the secret key rate for the scenario without secrecy constraints at relays, and then an XOR-based algorithm was proposed to generate a relay-oblivious key, (i.e., private key). In [12], a multi-antenna relay was considered to help the legitimate terminals to generate a secret key, and then the optimal attacker's strategy was characterized to minimize the secret key rate when Eve is an active attacker. The problem of private key generation is investigated in this paper. We consider a particular cooperative PIN model with M + 2 terminals (Alice, Bob, M relays) and an eavesdropper (Eve), where M ≥ 2. Under the help of relays, Alice and Bob wish to establish a private key which should be protected from not only Eve but also from individual relays simultaneously. One of the main contributions of this paper is to find the private key

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

capacity of this PIN model. To obtain the lower bound, we propose a novel algorithm for generating the private key. Specifically, using the observations at relays and the transmissions over the public channel, Alice and Bob first agree on M common messages, each of which is open to a certain relay. Then a random binning process is adopted in the key distillation step to map these insecure common messages into a private key. Such an algorithm is termed as the "RB-based algorithm" for simplicity. On the other hand, the upper bound of the private key capacity is obtained by considering M enhanced source models, each of which relaxes the secrecy constraints on some relays, and assumes that the relay observations are known by Alice or Bob in advance. Such an upper bound is tight and matches with the lower bound. The proposed RB-based private key generation algorithm in the PIN model can be extended to more practical wire- less communications. In particular, we consider a cooperative wireless network, in which Alice, Bob and the M relays use estimates of wireless channels as the correlative source observations. It is assumed that Alice and Bob are far away from each other, so there does not exist the direct link between Alice and Bob. Compared to the XOR-based algorithm in [11] whose multiplexing gain is ⌊M⌋/2 for the considered wireless network, the proposed RB-based algorithm achieves a larger multiplexing gain $M - 1$.

II. PAIRWISE INDEPENDENT NETWORK MODEL

Consider a DMS model, where Alice and Bob, with the help of $M \geq 2$ relays, wish to establish a private key that needs to be protected from Eve and individual relays simultaneously. All relays are assumed to be curious but honest: they will comply with the proposed transmission schemes for helping Alice and Bob to generate a key, but would also try to intercept the key information if they can [11]. The nodes can communicate to each other over a noiseless public channel whose capacity is infinite, but the transmitted information over the public channel is also available to Eve noisele,ssly. Eve is passive in the sense that it only receives but not transmits information.

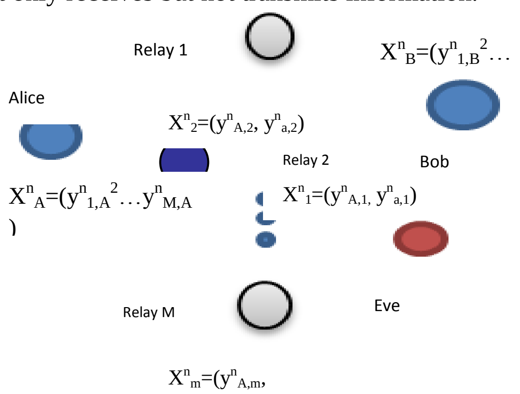


Fig 1. The considered cooperative PIN model with M relays

Pairwise independence does not imply mutual independence, as shown by the following example attributed to S. Bernstein. Suppose X and Y are two independent tosses of a fair coin, where we designate 1 for heads and 0 for tails. Let the third random variable Z be equal to 1 if exactly one of those coin tosses resulted in "heads", and 0 otherwise. Then jointly the triple (X, Y, Z) has the following probability distribution.

For $\forall m \in \{1,\cdots,M\}$, let $Y_{m,A}$ and $Y_{A,m}$ denote the cor- relative source observations at Alice and relay m, respectively. $Y_{m,B}$ and $Y_{B,m}$ denote the correlative source observations at Bob and relay m, respectively. Specifically, Alice observes n i.i.d. repetitions of random variable $XA = (Y_{1,A,}\cdots, Y_{M,A})$, denoted by $X_n^A = (Y^n{}_{1,A},\cdots,Y^n{}_{M,A})$; Bob observes n i.i.d. repetitions of random variable $XB = (Y_{1,B,}\cdots,Y_{M,B})$, denoted by $X^n{}_B = (Y^n{}_{1,B},\cdots,Y^n{}_{M,B})$; relay m observes n i.i.d. repetitions of random variable $X_m = (Y_{A,m},Y_{B,m})$, denoted by X_n m = (Y nA,m,YnB,m). This DMS model is a PIN in the sense that $I(Y_{i,\alpha},Y_{\alpha,i};\{Y_{j,\beta},Y_{\beta,j} : (j,\beta)\ 6\neq (i,\alpha)\}) = 0,$

for $i,j \in \{1,\cdots,M\};\alpha,\beta \in \{A,B\}$. (1)

his means that Alice and relay m have access to a pair $(Y_{m,A},Y_{A,m})$ which is independent of any other pair of source observations, so is $(Y_{m,B},Y_{B,m})$. Note that there does not exist correlated source observations between Alice and Bob, the private key can be generated only via the help from the relays. Moreover, we do not consider correlated sources observed by any pair of relays, since the common randomness shared by any pair of relays cannot contribute to the private key rate. More definitions are given as follows.

Without loss of generality, assume that the nodes use the public channel to communicate in a round robin fashion over q rounds. Let $1 \leq l \leq q$ and $1 \leq m \leq M$. Specifically, relay m transmits during rounds l that satisfy l mod (M+2) = m; Alice transmits during rounds l that satisfy l mod (M + 2) = M + 1; Bob transmits during rounds l that satisfy l mod (M + 2) = 0.

A (2n ˜ R1,··· ,2n ˜ Rq) code for the cooperative key gener- ation problem consists of :

(i) M + 2 randomized encoders, one for each node. In rounds l satisfying l mod (M + 2) = m, relay m generates an index $Fl \in \{1,\cdots,2n\ \tilde{}\ Rl\}$ according to p(fl|xn m,fl−1); in rounds l satisfying l mod (M +2) =M + 1, Alice generates an index $Fl \in \{1,\cdots,2n\ \tilde{}\ Rl\}$ according to p(fl|xn A,fl−1); in rounds l satisfying l mod (M + 2) = 0, Bob generates an index $Fl \in \{1,\cdots,2n\ \tilde{}\ Rl\}$ according to p(fl|xn B,fl−1).

(ii) Two decoders, one for Alice (decoder 1) and the other for Bob (decoder 2). After receiving the q rounds of transmissions (i.e., Fq = {F1,··· ,Fq}) over the public channel, decoder 1 generates a random key KA according to $KA = KA(X_{nA},Fq)$; Decoder 2 generates a random key KB according to $KB = K_B(X_nB,Fq)$.

A private key rate R is said to be achievable if there exists a $(2_n\ \tilde{}\ R_1,\cdots,2_n\ \tilde{}\ Rq)$ code such that

$$\Pr(K_A \neq K_B) \leq \varrho, \quad (2)$$

$$1/\ n\ H(KA) \geq R - \varrho, \quad (3)$$

$$1/\ n\ H(K_A) \geq 1/\ n\ \log|K_A| - \varrho, \quad (4)$$

$$1/\ n\ I(K_A;X_n{}^m,F^q) \leq \varrho, \text{ for } \forall m \in \{1,\cdots,M\}, \quad (5)$$

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

where $|K_A|$ denotes the size of the alphabet of the key K_A. Note that the secrecy constraints in (5) implies that the relays are assumed to be non-colluding.

The private key capacity CK is the supremum of all achievable rates R. $C_{(d)}$ K is used to denote the private key capacity with deterministic encoding and key generation functions. According to [5], $C_{(d)\ K} = C_K$, which means that randomization is useless for key generation in the addressed source model.

III. PRIVATE KEY CAPACITY OF PIN MODEL

For simplicity, we first define

$$I_i = \min\{I(Y_{A,i},Y_{i,A}),\ I(Y_{B,i},Y_{i,B}),€\{1,\dots M\};\ (6)$$

Furthermore, these parameters are ordered according to $I(1) \le I(2) \le \cdots \le I(M)$. Then the private key capacity for the considered scenario is given in the following theorem. Theorem 1: For the considered PIN model with M relays, the private key capacity is given by

$$CK = \sum_{i=1}^{M} I_i - \max(\ m€\{1, \quad ,M\})\ \ (7)$$

$$I_m = \sum_{i=1}^{M} I_I \quad (8)$$

Proof: The achievability part is proved by a novel RB-based key generation algorithm that is based on two steps: key agreement and key distillation. In the key agreement step, Alice and Bob can agree on M common messages, each of which is revealed to a certain relay. In the private key distillation step, these common messages will be mapped into the final private key via a RB-based private-key codebook. The converse part is proved by deriving the upper bounds of M symmetric enhanced channels. Each of these enhanced channels relaxes the secrecy constraints and assumes Alice and Bob to be genie-aided (i.e., knowing part of the sources observed by the relays). The details of the proof will be provided as follows

A. Proof of Achievability Algorithm 1 briefly shows the achievable scheme that is based on two steps: key agreement and key distillation. Let $R_{A,i} = I(Y_{A,i},Y_{i,A}) - ϙ$, $R_{B,i} = I(Y_{B,i},Y_{i,B}) - ϙ$ for $1 \le i \le M$; $R_i = \min\{R_{i,A},R_{i,B}\} = I_i - ϙ$, and they are ordered according to $R(1) \le \cdots \le R(M)$. Besides, Rkey =PM−1 i=1 R(i).

Algorithm 1: Relay-oblivious Key Generation

• Alice and Relay i agree on a pairwise key $W_{A,i}$ from the correlated observations ($Y^{\ n}_{\ i,A}$,$Y_n\ _{A,i}$); Bob and Relay i agree on a pairwise key $W_{B,i}$ from the correlated observations ($Y_{\ n\ i,B,}$$Y_{n\ B,i}$), i = 1,···M.

• Relay i sends $W_{A,i} \oplus W_{B,i}$ over the public channel, so Alice and Bob can obtain both $W_{A,i}$ and $W_{B,i,}$ i = 1,···M. Then they will choose the one with a smaller size as the common message, denoted as Wi∈ Wi. Step 2: Key Distillation:

• In advance, randomly grouped all the sequences w_M in W_M into $2_n(R_{key-ϙ})$ bins each with equal amount of codewords. All the other nodes also know this private- key codebook.

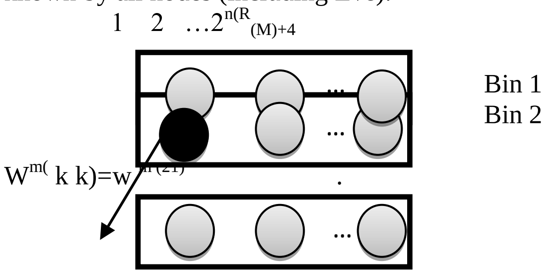
• Alice and Bob find the sequence $W_M = (W_1,\cdots ,W_M)$ in the RB based private-key codebook, and choose its bin number as the final private key.

Key Agreement: In the key agreement step, Alice and Bob will agree on M common messages. First, each relay i and Alice agree on a pairwise key $W_{A,i}$ using their correlated sources ($Y_{\ n\ A,i}$,$Y_{n\ i,A}$); each relay and Bob agree on a pairwise key using their correlated sources ($Y_{\ n\ B,i}$,$Y_{\ n\ i,B}$). According to the standard techniques [7] [2], each pairwise key $W_{A,i}$ ($W_{B,i}$) is generated using Slepian-Wolf coding and public transmission $F_{A,i}$ ($F_{B,i}$). Moreover, the pairwise keys $W_{A,i}$ and $W_{B,i}$ have the following properties [1], [2]: i) They can achieve the rates RA,i and RB,i, respectively; ii) They are uniformly distributed and can be decoded by both Alice and Bob correctly; iii) The pairs $\{(W_{\alpha,i},F_{\alpha,i})\alpha \in \{A,B\},i\in\{1,\cdots,M\}\}$ are mutually independent, due to the definitions of the PIN model. Second, each relay i sends out $W_{A,i} \oplus W_{B,i}$ over the public channel, so Alice and Bob can obtain both the two pairwise keys, and choose the one with a smaller size as the common message, denoted as Wi. Hence the rate of each common message Wi is Ri. According to [11], 1 n $I(W_1,\cdots ,W_M\text{-}F_q) \le ϙ1$. (9) 2) Key Distillation: In the key distillation step, both Alice and Bob map all the insecure common messages assembled from the key agreement step into the unique codeword in the private-key codebook, and set the bin number of this codeword as the final private key. Note that such a private-key codebookis generated based on random binning, so it provides necessary randomness such that the bin number is secret from all the relays and Eve.

Remark 1: The main difference between the proposed algorithm and the one in [11] lies in the key distillation step: the former is based on the RB process and the latter is based on an XOR process. In [11], Alice and Bob concatenate ($W_1 \oplus\ W_2,\cdots\ ,W_{M-1} \oplus\ W_M$) as the final private key in the key distillation step. Here M is assumed to be even.We will provide more details of the RB-based codebook in the following.

Codebook Generation

Let $w_i \in Wi = \{1,\cdots ,2_n^{\ Ri}\}$, $w_M = (w_1,\cdots ,w_M)$. Then, based on the concept of ran- dom binning, the private-key codebook can be constructed. Specifically, randomly and uniformly partition all the elements wM in set $W_M = W_1 \times W_2 \times \cdots \times W_M$ into 2n(Rkey−ϙ) bins each with $2n(R_{(M)}+ϙ)$ codewords. So each codewordwM can be indexed as $w_M(k,\tilde{\ } k)$, where $k \in \{1,\cdots ,2_n(Rkey-ϙ)\}$, $\tilde{\ } k \in \{1,\cdots ,2n(R(M)+ϙ)\}$. Fig. 2 illustrates the binning assign- ment for the private-key codebook, denoted by C, that is known by all nodes (including Eve).



ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering
ICITCSA 2017
Pioneer College of Arts and Science, Coimbatore
Vol. 6, Special Issue 1, January 2017

Fig. 2. The binning assignment for the private-key

codebook, where $w_M = (w_1,\cdots,w_M) \in WM$, $w_i \in \{1,\cdots,2_n^{Ri}\}$.

Decoding and key generation: Based on the common messages collected in the key agreement step, Alice and Bob can find their corresponding indices in the private-key codebook. Specifically, knowing $(W_1,\cdots,W_M)$, Alice finds the index pair (k,˜ k) from the private-key codebook such that w_M(k,˜ k) = $(W_1,\cdots,W_M)$. Then, it sets its key K_A = k. Similarly, Bob can also correctly find the key K_B = k. Since the error probability of the event that Alice and Bob share the same $(W_1,\cdots,W_M)$ is insignificant, the error probability $P(K_A$ 6= $K_B)$ is arbitrarily small as $n \to \infty$.

Analysis of the key rate: Since the private-key codebook is based on the random binning process, KA is uniformly distributed over {1,··· ,2n(Rkey−ϱ)} averaged over the code- book (i.e., C). Therefore, it can be obviously obtained that H(KA|C) = n(Rkey − ϱ).

Analysis of the secrecy constraints: For ∀m ∈ {1,··· ,M}, we will prove that the generated private key is secret from relay m. Define $W_M = (W_1,\cdots,W_M)$. Then, averaged over C, we have

$I(K_A;F_q,X_{nm}|C)(a) \leq I(K_A;Fq,W_m|C)$

$\leq I(K_A;W_m|C) + I(K_A,W_M;F_q|W_m,C)$

(b) $\leq I(K_A;W_m|C) + n\varrho 1 = I(K_A;W_m|C)$

where (a) is due to the fact that Xn m − (Wm,Fq) − KA is a Markov chain; (b) is due to (9) and the fact that KA is determined by WM for a given codebook. Furthermore,

$I(K_A;W_m|C)=I(K_A,W_M;W_m|C)-I(W_M;W_m|K_A,C)$

$=I(W_M;W_m|C)-H(W_M|K_A,C)+H(W_M|W_m,K_A,C)$

$=H(W_m|C)-H(W_M|K_A,C)+H(W_M|W_m,K_A,C)$.

For the first term, obviously we have $H(W^m|C) = n^{Rm}$. (12) Since $H(W_i|C) = n^{Ri}$, we have $H(W^M|C) = nP_M$ i=1 $_{R(i)}$. So the second term can be obtained as $H(W^M|K$
$A,C) = H(W^M|C) + H(K_A|W^M,C) - H(KA|C) = H(W^M|C) - H(K_A|C)$= n
M $_{X\ i=1}$
$R_{(i)} - n(Rkey - \varrho)= n(R^{(M)} + \varrho)$. (13)

The third term is bounded in the following lemma.

Lemma 2: When $R(M) = \max\{R_1,\cdots,R_M\}$ and n is sufficiently large, $H(W^M|W^m,KA,C) \leq n(R(M) - R^m + \delta(\varrho))$. (14)

Proof: This lemma can be proved using similar methods in existing related works, such as [13] (proof of Lemma 22.3) and [14], with some necessary variations. The details are omitted here due to space limitation. Combining (10) with (11), (12), (13) and (14), we have 1 n $I(KA;Fq,Xnm|C) \leq 1$ n $I(KA;W^m|C) + \varrho 1 \leq \delta(\varrho) + \varrho 1 - \varrho$. (15) So the private key rate Rkey =PM−1 i I(i) − ϱ is achievable. B. Proof of Converse The calculation of the upper bound is based on M symmetric enhanced channels. For the m-th enhanced source model, m = 1,··· ,M, we only consider the secrecy constraint on relay m, and ignore the secrecy constraints on all the other relays. Moreover, Alice and Bob are assumed to know the observations of two subsets of relays a priori, respectively. The definitions of the two subsets are given as follows. For a given m ∈ {1,··· ,M}, we will form two sets of nodes, i.e., A]m[and B]m[in the next. First, allocate Alice and Bob to A]m[and B]m[, respectively. Second, for relay i, i 6= m, if I(YA,i;Yi,A) > I(YB,i;Yi,B), allocate it to A]m[; otherwise, allocate it to B]m[. So I(YB,i;Yi,B) = min{I(YA,i;Yi,A),I(YB,i;Yi,B)} if relay i lies in A]m[, and I(YA,i;Yi,A) = min{I(YA,i;Yi,A),I(YB,i;Yi,B)} if relay i lies in B]m[. Then, assume without loss of generality that relays A1, A2, ···, Aj are allocated to A]m[, and relays B1, B2, ···, BM−1−j are allocated to B]m[, 0 ≤ j ≤ M − 11. Here {A1,··· ,Aj}T{B1,··· ,BM−1−j} = ∅ and {A1,··· ,Aj}S{B1,··· ,BM−1−j} = {1,··· ,m − 1,m + 1,··· ,M}. In other words, A]m[= {Alice, relays A1, ···, Aj}; B]m[={Bob, relays B1, ···, BM−1−j}. Now, by the max-flow principle [1], the max follow between the two sets A]m[and B]m[can be expressed as Pm i=1 Ii − Im, which is the upper bound of the m-th enhanced channel. Due to space limitation, the details are omitted here. Choosing the smallest bounds among all the M enhanced channels, we can obtain CK ≤PM i=1 Ii −maxm∈{1,···,M} Im.

IV. KEY GENERATION IN WIRELESS NETWORK

In this section, we will extend the RB-based algorithm proposed for the PIN model into the wireless network, and use the estimates of wireless fading channels as source observations for private key generation.

A. Model

The considered wireless network can be viewed as a practical example of the PIN model in Section II. All the nodes have a single antenna and are half-duplex constrained. In this wireless network, it is assumed that there is no direct link between Alice and Bob, since they are located far from each other. Denote hA,i (hB,i) as the fading channel gains between relay i and Alice (Bob). All channels are assumed to be reciprocal. It is reasonable to assume that all the fading channel gains and noise are random variables and independent of each other. An ergodic block fading model is considered, in which all the channel gains remain constant for a block of T symbols and change randomly to other independent values after the current block. For simplicity, we assume hA,i∼ N(0,δA,i), hB,i∼ N(0,δB,i). Moreover, none of the nodes knows the values of hA,i and hB,i a priori, but all the nodes know their statistics. Assume that terminals transmit in a time-division manner. For L channel uses, let Si = [si(1),··· ,si(Li)]T , SA = [sA(1),··· ,sA(LA)]T and SB = [sB(1),··· ,sB(LB)]T de- note the signals sent by relay i, Alice and Bob, respectively, where i = 1,··· ,M, and LA + LB +PM i=1 Li = L. For simplicity, we consider an equal power constraint for the legitimate terminals, that is 1 Li
E {ST i Si}, 1 LA E {ST ASA}, 1 LB E {ST BSB} ≤ P

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

B. Proposed RB-based Algorithm

Algorithm can be extended to wireless networks for private key generation. Briefly speaking, all the relays, Alice and Bob take turns to broadcast training sequences. After the channel estimation step, Alice and Bob will generate the private key using the RB-based scheme in Algorithm 1 (Section III). Now, we will explain the
1If j = 0, {A1,··· ,Aj} = ∅ and A]m[= {Alice};
if j = M − 1, {B1,··· , Bj} = ∅ and B]m[= {Bob}.
channel estimation step in more detail. Fig. 3 shows the time frame for the training of the proposed scheme in each fading block. Each fading block is divided into M +2 time slots, and the numbers of symbols in these time slots are T1,··· ,TM, TA, TB, respectively, where TA+TB+PM i=1 TM = T. Suppose relay i, Alice and Bob sends known training sequences Si of size 1 × Ti, SA of size 1 × TA and SB of size 1 × TB, respectively. The energy of each sequence is ||Si||2 = TiP, ||SA||2 = TAP, ||SB||2 = TBP, where || · || denotes the Euclidean norm.

From n fading blocks, Alice can obtain the estimates(˜ hn 1,A,··· ,˜ hnM,A); Bob can obtain the estimates (˜ hn 1,B,··· ,˜ hnM,B); relay i can obtain the estimates (˜ hnA,i,˜ hnB,i), i = 1,··· ,M. These estimates are noisy versions of the corresponding fading channels. The details of this channel estimation step are omitted here due to space limitation, and similar works can be found in [11], [12]. The rate of each pairwise key Wα,i can be calculated as RG α,i =1 2
log 1 + TiTαP2δ4α,i δ4 + (Ti + Tα)δ2δ2α,iP!, ∀α ∈ {A,B},i ∈ {1,··· ,M}, (17) where δ2 is the variance of each Gaussian noise. Now, using the result in Theorem 1, the proposed RB-based algorithm achieves the private key rate RG key for some tuple (TA,TB,T1,··· ,TM), which can be written as
RG key =1 T M X i=1
IG i − max i∈{1,···,M}
IG i !, (18)
with IG i = min{RG A,i,RGB,i}. To further show the impact of the proposed scheme on the gain of the key rate, the multiplexing gain (introduced in [11]) is analyzed as following. Corollary 3: For the considered wireless network with M relays, the multiplexing gain of the private key rate achieved by the proposed RB-based algorithm is M − 1. Proof: Based on the definition of in [11], the multiplexing gain of the proposed algorithm should be limP→∞ RGkeyRs , where Rs ≈ 1 2T logP as P → ∞. From Eq. (17), it is easy to obtain that limP→∞ RG α,iRs = T, so we have limP→∞ RGkeyRs = M − 1.

Remark 2: If there are no secrecy constraints at the relays, the multiplexing gain is M [11]. So the proposed RB-based algorithm sacrifices one multiplexing gain for satisfying the secrecy constraints at all the M relays. This loss is insignificant because only one multiplexing gain is sacrificed, no matter how large M is. But for the XOR-based algorithm in [11] (Corollary 10), its multiplexing gain is ⌊M/2⌋ if there does exist the direct link between Alice and Bob. Therefore this existing scheme suffers a loss of M/2 multiplexing gain in comparison with the case without secrecy constraints at the relays. Hence the proposed RB-based scheme can effectively enhance the performance of the private key generation.

V. CONCLUSION

In this paper, we have investigated the problem of private key generation. A particular cooperative PIN model with M+2 terminals is considered, where Alice, Bob and M relays observe pairwise independent sources. Under the help of relays, Alice and Bob wish to establish a private key that is secure from Eve and all relays. The private key capacity of this PIN model has been found. The achievability is proved via a novel RB-based algorithm for generating the private key. The upper bound of the private key capacity is obtained by considering M enhanced source models. Then, we further consider a cooperative wireless network, in which estimates of wireless channels are regarded as the correlative source observations. Compared to the XOR-based algorithm in [11] whose multiplexing gain is ⌊M⌋/2, the proposed RB-based algorithm achieves a larger multiplexing gain M − 1.

REFERENCES

[1] C. Ye and A. Reznik, “Group secret key generation algorithms,” in IEEE International Symposium on Information Theory, 2007, pp. 2596–2600.
[2] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, “Secret key generation for a pairwise independent network model,” IEEE Transac- tions on Information Theory, vol. 56, no. 12, pp. 6482–6489, 2010.
[3] L. Lai and S.-W.Ho, “Simultaneously generating multiple keys and multi-commodity flow in networks,” in IEEE Information Theory Work- shop (ITW), 2012, pp. 627–631.
[4] L. Lai and L. Huie, “Simultaneously generating multiple keys in many to one networks,” in IEEE International Symposium on Information Theory Proceedings (ISIT), 2013, pp. 2394–2398.
[5] I. Csisza´r and P. Narayan, “Common randomness and secret key gener- ation with a helper,” IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 344–366, 2000.
[6] “Secrecy capacities for multiple terminals,” IEEE Transactions on Information Theory, vol. 50, no. 12, pp. 3047–3061, 2004.
[7] R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography.part i: secret sharing,” IEEE Transactions on Information Theory, vol. 39, no. 4, 1993.
[8] D. Tse and P. Viswanath, Fundamentals of wireless communication. Cambridge university press, 2005.
[9] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, “Information-theoretically secret key generation for fading wireless chan- nels,” IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 240–254, 2010.
[10] Q. Wang, K. Xu, and K. Ren, “Cooperative secret key generation from phase estimation in narrowband fading channels,” IEEE Journal on Selected Areas in Communications, vol. 30, no. 9, pp. 1666–1674, 2012.
[11] L. Lai, Y. Liang, and W. Du, “Cooperative key generation in wireless networks,” IEEE Journal on Selected Areas in Communications, vol. 30, no. 8, pp. 1578–1588, 2012.
[12] H. Zhou, L. Huie, and L. Lai, “Secret key generation in the two-way relay channel with active attackers,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 3, pp. 476–488, 2014.
[13] A. El Gamal and Y.-H. Kim, Network information theory.Cambridge University Press, 2011. [14] H. Zhang, L. Lai, Y. Liang, and H. Wang, “The capacity region of the source-type model for secret key and private key generation,” IEEE Trans. Information Theory, vol. 60, no. 10, pp. 6389–6398, Oct 2014.