Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 2, February -2015

INFORMATION THEORETIC TECHNIQUE FOR EFFECTIVE KEY GENERATION

S.SUGANTHI [1] A. MALATHI [2] ANAND JOSEPH DANIEL[3], D. RAJINI GIRINATH [4]

PG Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India,suganthiselvam90@gmail.com

Assistant Professor, Department of Computer Science and Engineering Anand Institute of Higher Technology, Chennai, Tamil Nadu , India, 2malathiarunachalam83@gmail.com

Assistant Professor, Department of Computer Science and Engineering Anand Institute of Higher Technology, Chennai, Tamil Nadu , India, 3danny02.2009@gmail.com

Head of Department, Department of Computer Science and Engineering Anand Institute of Higher Technology, Chennai, Tamil Nadu, India,4aiht.csehod@gmail.com

Abstract-*The two way relay channel, in which twoterminals are connected through a relay. The basic idea of two way relay channel schemes is to create a virtual direct link between two terminals can obtain channel estimates. Wireless fading channels need the direct wireless link between two terminals for generating key attributes. The proposed model consists of the key generation in the two-way relay channel that two terminals involved do not need to obtain correlated estimates. The relay first establishes a pair-wise key by using channel link. Higher rated key is generated by using an effective key generation scheme, so that the active attackers do not know any information and it helps in achieving a substantially larger key rate than that of a direct channel mimic approach. The two way relay channel need any correlation between two terminals. There is no need of any correlations between nodes in proposed scheme. Active attacker strategy that minimizes the key rate of the proposed scheme and have established the maximal attacker's power under which our scheme can still achieve a non-zero key rate.*

Keyword*—Active attack, information-theoreticsecurity, key generation, two-way relay channel.*

I. INTRODUCTION

Network security refers to any activities intended to defend the network. Specifically, these activities provides the usability, trustworthiness, truthfulness, and safety of the network and data. Actual network security targets a variety of threats and stops them from entering or spreading on your network.In certain applications, two terminals might be far away from each other, and hence there is no direct channel between them. The two-way relay channel, in which two terminals are connected through a relay. The key generation from the two way relay channel problem was considered in which proposed several interesting schemes to circumvent the issue that there is no direct channel to provide the necessary common randomness. The basic idea of these schemes is to create a virtual direct link from which these two terminals can obtain channel estimates.

In the proposed model, a new scheme for the key generation in the two-way relay channel by adopting a scheme proposed instead of trying to mimic a direct channel .In this, the two terminals involved do not need to obtain correlated estimates. Instead, the relay first establishes a pair-wise key with sender using the physical channel linking it and sender. Similarly, the relay and receiver can establish a pair-wise key using the channel linking them. Then the relay transmits the XOR of these two pair-wise keys to both sender and receiver. sender and receiver can then decode both keys and pick the one with a smaller size as the final key. The advantages of this approach are: 1) attacker does not obtain any information about the key generation, hence the scheme helps in obtains a much higher key rate; 2) It is very easy to evaluate the key rate 3) It can be extended to multiple antenna case. The other main contribution of this scheme is to consider the active attacker scenario.

The anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management. Several security schemes for data sharing on untrusted store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.

II. RELATED WORK

The basic idea of two way relay channel schemes is to create a virtual direct link between two terminals can obtain channel estimates. These two channel gains can serve as the common randomness for the secret key generation. Sender sends the trained sequence. But tampered sequence is received to destination nodes by modifying the active attackers for the usage of direct secret key generation [1]. In cooperative communications, the received information at the intended destination node depends largely on the information received by some intermediate, possibly untrusted, relay nodes [2]. Here the secret key generation has been studied for a classical three-node cooperative wireless communication system with passive adversaries.

In particular, it is shown that such secret key agreement is possible for a scenario where all three parties receive the output of a binary symmetric source over independent binary symmetric channels [3], even when the enemy's channel is superior to the other two channels. The results suggest how to build cryptographic systems that are provably secure against enemies with unlimited computing power under realistic assumptions about the partial independence of the noise on the involved communication channels**.** Information-theoretic or unconditional security is more desirable in cryptography than computational security for two reasons. First, for the former no assumption about the enemy's computing power is needed, and second, perfect secrecy is unarguable the strongest definition of security and hence the justification of a weaker definition of security is avoided.

The multipath-rich wireless environment associated with typical wireless usage scenarios is characterized by a fading channel response that is with time variation, sensitive to location, and distinctively shared by a given sender and receiver pair. The complexity associated with a richly scattering environmentimplies that the short-term fading process is inherently hard to predict and best shown stochastically, with rapid decorrelation properties in space, time and frequency. Here determine how the channel state between a wireless sender and receiver can be used as the basis for building practical secret key generation protocols between two entities [5].So begin by presenting a scheme based on level crossings of the diminishing process, which is well-suited for the Rayleigh and Rician fading models associated with a richly scattering environment.

The level crossing algorithm is modest, and integrates a self-authenticating mechanism to prevent oppositional manipulation of message exchanges during the protocol. Since this algorithm is best suited for diminishing processes that exhibit balance in their underlying distribution, the second and more prevailingmethod that is suited for more general channel state distributionsis driven by the observation from quantizing jointly Gaussian processes, but achievesexperimental measurements to set quantization boundaries and aexperimental log probability ratio estimate to achieve an improved secret key generation rate is avoided.

III. MODEL

The simplest model consists of two way relay channel consists of sender, receiver, relay and attacker is represented here.There exists no correlation between the sender and the receiver. The constructs representing sender transmitting signal x_s to the receiver in the presence of an attacker is,

$$Z_r = h_{sr} x_s + y_1 + m_r, \quad (1)$$

$$z_a = h_{as} x_s + m_a, \quad (2)$$

Where h_{sr} represents fading coefficient of the channel from sender to relay, y_1 is the attack signal to attacker, m_r is the Gaussian noise. h_{as} is the channel gain between sender and the attacker, m_a, is the noise at attacker.

Similarly, Receiver sends the signal x_r, to the sender as follows,

$$Z_r = h_{Cr} x_c + y_2 + m_r, \quad (3)$$

$$z_a = h_{ca} x_c + m_a, \quad (4)$$

Where h_{Cr} represents fading coefficient of the channel from receiver to relay, y_2 is the attack signal to attacker, m_r is the Gaussian noise. h_{ca} is the channel gain between receiver and the attacker, m_a, is the noise at attacker.

IV. PROPOSED WORK

The two terminals are involved that do not need to obtain correlated estimates between the two terminals. The relay first establishes a pair-wise key for security strategies. It can establish the active attacker's strategy for more secure approaches are generated.

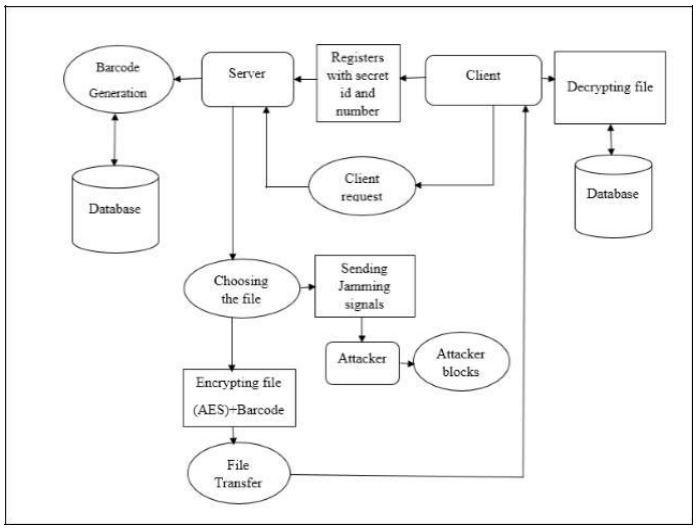


Figure 1: Overall Process Diagram for effective key rate

The optimal attacker's strategy that minimizes the key rate of the proposed scheme. Furthermore, it enables the maximal attacker's power under which our scheme can still achieve a nonzero key rate**.** Instead of using static single antennas, the pair-wise key establishes their channel link to multiple antennas. It validates the effectiveness of using multi-level quantization when there is enough mutual information in the channel. If an eavesdropper has multiple antennas, attacker cannot gain much more information about the legitimate channel and have the following advantages.

1) Attacker does not obtain any information about the channel gains used for the key generation and it obtains a much higher key rate.
2) It is very easy to evaluate the key rate.

ALGORITHM DESIGN

Step 1: Begin.
Step 2: All authorised users registered with theirunique secret id and number to the admin of the corresponding network.
Step 3: The Scenario, is considered with the activeuser.
Step 3.1: The authorised user request for the data tothe admin.
Step 3.2: The admin verifies the authorised user withtheir unique secret id and number.
Step 4: Sending jamming signals to the attacker
Step 4.1: The active attacker is waiting to corrupt therequired data of the client requested.
Step 4.2: To preventing that, the admin first sendingthe jamming signals with the duplicate data to all the active attackers.
Step 4.3: Having the probabilistic calculation of timeof jamming signal, the admin checks for client active state and send the encrypted data.
Step 5: Setting path key
Step 5.1: For the more security of data ,the path key isset in the path through which the data is passed.
Step 6: From the above all steps we can achieve theeffective key rate in the presence of active attackers.
Step 7: End

V. IMPLEMENTATION

The two-way relay channel, in which two terminals are connected through a relay, is a basic setup that models this scenario. The key generation from the two way relay channel problem was considered in, which proposed several interesting schemes to circumvent the issue that there is no direct channel to provide the necessary common randomness. The basic idea of these schemes is to create a virtual direct link from which these two terminals can obtain channel estimates and then apply the approach in.There is an increasing need for sharing information across autonomous entities in such a way that no information apart from the answer to the query is

revealed. It formalizes the notion of minimal information sharing across private database and develops protocols for joint, equijoin, joint size, and equijoin size. A new scheme for the key generation in the two-way relay channel by adopting a scheme proposed in our recent work. Instead of trying to mimic a direct channel as done in, in the proposed scheme, the two terminals involved do not need to obtain correlated estimates. Instead, the relay first establishes a pair-wise key with user1 using the physical channel linking it and user2. Similarly, the relay and user1 can establish a pair-wise key using the channel linking them.

The key privacy properties that the protocol for privacy-preserving Classifier learning must guarantee are, informally, as follows. First, the records from which the classifier is constructed should remain confidential from the party who obtains the classifier (except for the information which is inevitably revealed by the classifier tree itself). Second, the data owner should not learn anything about the classifier which has been constructed. The algorithm for constructing the classifier is standard , if the classifier is being constructed only on a subset of database records. The user's protocol output is a classification tree constructed from the Server's data. The server learns nothing from the protocol; in particular, it does not learn the parameters of the classification algorithm, not even which attributes have been used when constructing the classifier.

Implementation is done with the main process such as, preventing active attackers.

Adding more security features

1) Key generation for encrypting and decrypting data.
2) Providing unique Id-Barcode.
3) Providing secure path code.

Sender:

Step1: Authorized users are registered with their user id and secret number.

Step2: Piggyback is done to confuse the active attackers. Providing the jamming signals to the attackers.

Step3: Making attackers busy, original data is uploaded for the authorized receiver.

Step4: Adding more security features,

1) Dynamic validation of barcode.
2) Providing secure path code.

Attacker:

Step1: Once the data is uploaded by the authorized user in the sender part, the attacker brings to listen mode.

Step2: Piggyback is done to confuse the attacker.

Fake data is uploaded with the same process which is done for transferring the original data to the authorized user in the receiver part.

Receiver:

Step1: When the data arrives at the receiver side it is stored in the target location.

Step2: The data is decrypted with the appropriate key and unique id.

VI. MATHEMATICAL MODEL

Consider the column to be the polynomial in GF (28) domain, and multiplies the fixed polynomial a (s) given below.

B(s) = {01}s3+{02}s2+{02}s+{03}

This formula in matrix multiplication as follows,

Consider A' (s) = c (s) ·d(s),

$$\begin{bmatrix} A'_{0e} \\ A'_{1e} \\ A'_{2e} \\ A'_{3e} \end{bmatrix} = \begin{vmatrix} 01 & 01 & 03 & 01 \\ 02 & 02 & 01 & 03 \\ 03 & 01 & 02 & 01 \\ 01 & 03 & 02 & 01 \end{vmatrix} \times \begin{bmatrix} A'_{0e} \\ A'_{1e} \\ A'_{2e} \\ A'_{3e} \end{bmatrix}$$

The result of multiplication in one column is expressed as,

A′0，e=({01}· A0，e)⊕({02}· A1，e)⊕A2，e⊕A3，e)

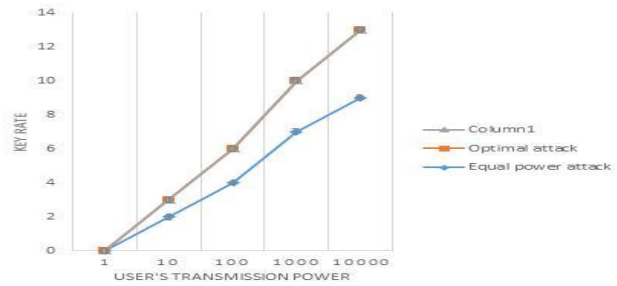
A′1,e= (A0，e⊕({01}· A1，e)⊕({01}·A2，e)⊕A3，e)

A′2,e= (A0，e⊕A1，e⊕({01}·A2，e)⊕({02}· A3，e)

A′3,e= ({02}·A0，e)⊕A1，e⊕A2，e⊕({03}· A3，e)

VII. SIMULATION AND RESULTS

Compare the key rate with optimal attack power and equal power strategy. Solve with the simple values by taking the user's transmission from the range of 1 to 1000 and varying key values.



VIII. CONCLUSION

The proposed effective key generation scheme achieves a considerably larger key rate than that of a direct channel mimic method. In distinct prevailing schemes, there is no need for the key generating terminals to obtain correlated observations. Also investigated the effects of an active attacker on the proposed key generation protocol. By characterizing the optimal attacker's strategy, it minimizes the key rate of the proposed scheme and have established the maximal attacker's power under which our scheme can still achieve a non-zero key rate. The description of differentially private algorithms assume an ideal model of computation: real systems require additional security assumptions that have to be verified. The difference between truly random noise and pseudo randomness and the effects of finite precision can lead to a gap between the theoretical ideal and practice. Numerical optimization methods used in some privacy methods can only produce approximate solutions; they may also have complex termination conditions unaccounted for in the theoretical analysis. MCMC sampling is similar. If we can guarantee that the sampler's distribution has total variation distanced from the Bingham distribution, then sampler can guarantee differential privacy. However, we do not yet have such analytical bounds on the convergence rate; we must determine the Gibbs sampler's convergence empirically.

REFERENCES

[1] Chung Chan and LizhongZheng**(**June 2014), "Multiterminal Secret Key Agreement"**,** IEEE transactions on information theory, Vol. 60, no. 6, pp.3380-3398.

[2] Ning Wang, Ning Zhang, T. Aaron Gulliver, (February 2014**) "**Cooperative Key Agreement for Wireless Networking:Key Rates and Protocol Design" IEEE transactions on information forensics and security, Vol. 9, no. 2, pp.272-280.

[3] Lifeng Lai,Yingbin Liang, H. Vincent Poor (April 2012.),**"**A Unified Framework for Key Agreement over WirelessFading Channels", IEEE transactions on information forensics and security, Vol. 7, no. 2, pp.481-489.

[4]Pengfei Huang, Xudong Wang, Shanghai Jiao, (**2013**) "Fast Secret Key Generation in Static Wireless Networks: A Virtual Channel Approach", Proceedings IEEE INFOCOM, pp.2293-2300.

[5]Francesco Renna, Matthieu R. Bloch, Nicola Laurenti,(February2013),**"**Semi-Blind Key-Agreement over MIMO Fading Channels", IEEE transactions on communications, Vol. 61, no. 2,pp.620-625.

[6] KanapathippillaiCumanan, Zhiguo Ding, Bayan Sharif, Gui Yun Tian,and Kin K. Leung,(May 2014), "Secrecy Rate Optimizations for a MIMO Secrecy Channel With a Multiple-Antenna Eavesdropper",IEEE transactions on vehicular technology, Vol. 63, no. 4,pp.1680-1686.

[7] H. Zhou, L. Huie, and L. Lai (Mar. 2013), "Key generation in two-way relay wireless channels," in *Proc. 17th Annu.Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, pp. 1–6.

[8] K. Ren, H. Su, and Q. Wang (August 2011), "Secret key generation exploiting channelcharacteristics in wireless communications,"IEEEWirelessCommunications, vol. 18, pp. 6–12.

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

[10] J. Muramatsu, K. Yoshimura, and P. Davis, "Secret key capacity and advantage distillation," in *Proc.* IEEE Int. Symp. Inf. Theory, Jul. 2006, pp. 2598–2602.

