Privacy Preserving of Data Sharing for Cooperative Network with Untrusted Relay Nodes

Deepthi Mai Karanam[1], Behara Vineela[2]

[1]*Final M.Tech Student,* [2]Asst.professor

[1,2]Dept of CSE, *Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh*

Abstract: *one of the fundamental goals of network is to provide security of sharing information. Before sharing the information in network each node will be identified by server for the authentication. By providing authentication process we can identify the nodes trusted or untrusted. If the node is trusted node it will share information through the network. But the node is untrusted node it will jamming transferred message. By performing authentication process we can generate signature of each node in the network. By verifying the signature it will conform the given node is trusted node or untrusted node. In this paper we are proposed mainly two concepts for authentication of nodes in network and privacy of transferring message. In this paper we are using prime order signature algorithm for the generation of signature and bit level key xor algorithm for encryption, decryption of transferring message. By implementing the prime order signature algorithm we can find out node is trusted node or untrusted node in a network. By using bit level key xor algorithm we can convert transferring message into unknown format and again get convert unknown format data into plain format. By implementing those techniques we can provide more efficiency and more privacy of transferring message.*

Keywords: *Security, Cryptography, Jamming, Signature, secret key*

I. INTRODUCTION

Information theoretic security was proposed of measuring secrecy using mutual information lends itself naturally to the investigation of how the channel can influence secrecy and further to the characterization of the fundamental limit of secure transmission rate. Recent progress in this area has extended classical information theory channel models to include secrecy constraints. Examples are the multiple access channel, the broadcast channel, the two-way channel, the three-node relay channel and the two-user interference channel [1–9]. These studies are beginning to lead to insights for designing secure wireless communication systems from the physical layer up. The focus of this work is on a class of relay networks where the source and the destination have no direct link and thus can only communicate utilizing an intermediate relay node. This models the practical scenario where direct communication between the source and the destination is too "expensive" in terms of power consumption: direct communication may be used to send some very low rate control packages, for example to initialize the communication, but it is infeasible to sustain a nontrivial reliable communication rate due to the power constraint. In such a scenario, the source-destination pair needs the relay to communicate. On the other hand, more often than not, this relay node may be "untrusted" [6]. This does not mean the relay node is malicious, in fact quite the opposite, it may be part of the network and we will assume that it is willing to faithfully carry out the designated relaying scheme. The relay simply has a lower security clearance in the network and hence is not trusted with the confidential message it is relaying.

Equivalently, we can assume the confidential message is one used for identification of the source node for authentication, which should never be revealed to a relay node in order not to be vulnerable to an impersonation attack. In all these cases, we must assume there is an eavesdropper collocated at the relay node when designing the system. The "untrusted" relay model, or the eavesdropper being collocated with the relay node, was first studied in [5] for the general relay channel, with a rather pessimistic outlook, finding that for the degraded or the reversely degraded relay channel the relay node should not be deployed. More optimistic results for the relay channel with a collocated eavesdropper have been identified recently in [6, 10, 11]. Specifically, it has been shown that the cooperation from the relay may, in fact, be essential to achieving nonzero secrecy rate [6, 11]. The model is later extended to the more symmetric case in [12, 13] where the relay also has a confidential message of its own, which must be kept secret from the destination. All these models assume that a direct link between the source and the destination is present including our previous work [5]. In contrast, when there is no direct link, it is impossible for this network to convey a confidential message from the source to the destination while keeping it secret from the relay [6]. This is because the destination can only receive signals from the relay resulting in a physically degraded relay channel [14]. Therefore, the relay knows everything the destination knows regarding

the confidential message, and the secrecy capacity is zero.

The paper is organized as follows. Section 2 presents the related work of our proposed system. In Section 3, implementation procedure of our proposed system. Section 4 conclusion of this paper. Section 5 presents references of our proposed system.

II. RELATED WORK

The research on untrusted relay systems was pioneered by He and Yener in [15], where the non-zero secrecy rate is proven to be achievable by enlisting the help of the destination who performs jamming. In [16], the joint beam forming design at the source and the relay was proposed for MIMO untrusted relay systems. In [17], the secrecy outage probabilities of several relaying schemes were analyzed. In [18], the power allocation policy was developed for amplify-and-forward (AF) untrusted relay systems. Although diverse results on untrusted relay systems have been reported, the majority of existing works deal with the simple model with only one relay node. For multi-relay networks, [19] analyzed the relationship between the system secrecy capacity and the number of untrusted relays. Reference [20] proposed to use relay assignment and link adaptation to realize both secure and spectral-efficient communications. However, [19] and [20] only considered the information leakage problem during the first phase of any two-hop transmission. This simplifies the protocol design, but may not hold in practice. Unlike [19] and [20], we in this paper try to secure the transmissions of both the first and the second phases, and our contributions are threefold: First, an alternate jamming method is introduced to prevent information leakage. Second, both optimal and sub-optimal secrecy-enhanced relay selection policies are proposed. Third, the lower bound of the achievable ergodic secrecy rate (ESR) is derived, and the asymptotic analysis of the ESR is given as well.

III. PROPOSED SYSTEM

Cooperative networks are more attention for sharing of information with secure manner. Before providing security of transferring message the cooperative network will find out the nodes are trusted nodes or untrusted nodes. Because the network contains more than one node can be perform sharing of information between them. So that the information can be sent to trusted party only and untrusted party will not get that information. So that before transferring message or information the cooperative network will perform the authentication process for finding available nodes are trusted nodes or untrusted nodes in a network. After that the cooperative network only sent information between the trusted nodes. If any untrusted nodes will try to get the information it will stop or jamming information. In this paper we are using prime order signature algorithm for finding trusted nodes or untrusted nodes in a network. After finding that we are using bit level key xor algorithm for encryption and decryption of transferring message. The implementation procedure of prime order signature algorithm is as follows.

Prime order signature algorithm:

In this module each node will generate signature using the prime order signature algorithm and sent those signatures to server. The generation of signature is as follows.

1. Each node (n_i) will choose two prime numbers P,Q and calculate N= P * Q
2. After calculating the node again chooses another random number b the range between the N.
3. By using those values each node will generate private key and public is given below.

   Public key is (N , b) and private key is(P, Q)

4. Each node will choose random padding U and calculate H(ID* U)
5. After that each node will solve the following equation.

   X^2 = H (ID * U) mod N where H is one way hash function.
6. Each node will generate signature m is the pair(U,X).

7. The server a will retrieve the message *m* and a signature *(U,x)* the verifier *V* calculates *x*2 and *H(mU)* and verifies that they are equal the node are authenticated else not authenticated.

After find out trusted nodes or untrusted nodes the server will sent the status to each node in the network. After that the server will choose secret key randomly and sent that key to all nodes in the network. The trusted nodes will retrieve secret key and using that key we perform the encryption and decryption of transferring message. The encryption and decryption process of bit level key xor algorithm is as follows.

Bit level key xor algorithm:

i. Encryption process:

1. Retrieve the secret key sent by the server in the network

2. Convert secret key into 16 bit binary format.

3. Pick the characters one by one from the plain text and convert those characters into ASCII format.

4. Performing xor operation of between key and message.
5. After performing xor operation we can reverse the total binary format of xor values.

6. Taken the reversed binary data and split into equal parts.

7. Perform the reverse operation on both parts and get reversed binary format data.

8. The reversed binary parts can be convert into ascii format and again perform xor between two parts.

9.after performing xor operation the result ascii value can be convert into binary format.
10. combine both binary data of first block and xored binary data.

11. That binary data sent to specified destination node in the network.

Before sending cipher format data to destination node the source node will generate signature of cipher format data. After generating signature the source node will sent signature and cipher format to destination node.

ii. Decryption process:

The destination node will retrieve the cipher format and signature. After retrieving signature and cipher format the destination node again generate signature for cipher data. After that compare both signatures, if the signatures are perform the decryption process of bit level key xor algorithm. If both signatures are not equal we can jam message.
The decryption process of bit level key xor algorithm is as follows.

1. The destination node will retrieve the cipher format data.

2.split the cipher format data into two parts and convert into ascci format.

3. xor both values and convert into binary format.

4.after converting perform the reverse operation on first block and xored binary data.

5. combine the both first block and xor data.

6.after combining again we can perform the reverse operation on combined data.

7.after completion of reverse process we can convert into ascii format.

8.retrieve secret key sent by server and perform xor operation between secret key and ascii value.

9.after completion of xor operation we can get original plain format data.

IV. Conclusions

In this paper we have proposed concepts for cooperative communication between nodes in a wireless sensor network. By implementing the proposed concepts we can effectively identify the nodes are trusted nodes or untrusted nodes. Because only the trusted nodes will share information in wireless sensor network. Other nodes will not get any information and it will jamming transferred message in a wireless sensor network. In this paper we are proposed two concepts for finding trusted or untrusted nodes in a wireless sensor network. Another concept is providing security of transferring message in a network. Before transferring message from source node to destination node each node will identify the server for the status of trusted node or untrusted node. By performing authentication process in this paper we are proposed concepts prime order signature algorithm. After finding trusted nodes each node will perform the encryption process for using bit level key xor algorithm. After completion of encryption process the source node will sent cipher format information to destination node. The destination node will retrieve the cipher format data and decrypt the data by using decryption process of bit level key xor algorithm. By implementing those concepts we can improve the efficiency of wireless network and also provide more privacy of transferring message.

V. REFERENCES

[1] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," IEEE Transactions on Information Theory, vol. 54, no. 3, pp. 976–1002, 2008.

[2] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in Proceedings of the 39th Asilomar Conference on Signals, Systems and Computers (ACSSC '05), pp. 1747–1751, Pacific Grove, Calif, USA, October-November 2005.

[3] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," IEEE Transactions on Information Theory, vol. 54, no. 12, pp. 5747–5755, 2008.

[4] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2735–2751, 2008.

[5] Y. Oohama, "Relay channels with confidential messages," submitted to IEEE Transactions on Information Theory http://arxiv.org/abs/cs/0611125.

[6] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," IEEE Transactions on Information Theory, vol. 54, no. 9, pp. 4005–4019, 2008.

[7] X. He and A. Yener, "Cooperation with an untrusted relay: a secrecy perspective," 2008, submitted to IEEE Transactions on Information Theory http://arxiv.org/abs/0910.1511.

[8] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confi- dential messages: secrecy rate regions," IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2493–2507, 2008.

[9] R. Liu and H. V. Poor, "Multi-antenna Gaussian broadcast channels with confidential messages," in Proceedings of IEEE International Symposium on Information Theory (ISIT '08), pp. 2202–2206, Toronto, Canada, July 2008. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[10] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in Proceedings of the 41st Asilomar Conference on Signals, Systems and Computers (ACSSC '07), pp. 883–887, Pacific Grove, Calif, USA, November 2007.

[11] X. He and A. Yener, "The role of an untrusted relay in secret communication," in Proceedings of IEEE International Symposium on Information Theory (ISIT '08), pp. 2212–2216, Toronto, Canada, July 2008.

[12] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in Proceedings of IEEE International Symposium on Information Theory (ISIT '08), pp. 2217–2221, Toronto, Canada, July 2008.

[13] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," 2008, submitted to IEEE Transactions on Information Theory http://www.ece.umd.edu/ ulukus/ papers/journal/crbc-secrecy.pdf.

[14] T. M. Cover and A. A. El Gamal, "Capacity theorems for the relay channel," IEEE Transactions on Information Theory, vol. 25, no. 5, pp. 572–584, 1979.

[15]. X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[16].C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming designvat the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[17] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenrative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[18] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–292, Jun. 2014.

[19] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[20] H. Khodakarami and F. Lahouti, "Link adaptation with untrusted relay assignment: Design and performance analysis," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4874–4883, Dec. 2013.

BIOGRAPHIES:

Karanam Deepthi Mai , is student in M.Tech(CSE) in Sarada Institute of Science Technology and Management, Srikakulam. She has received her B.Tech(IT) from Sarada Institute of Sscience Technology and Management,Srikakulam. she is interesting areas are datamining and network security

Behara Vineela is working as Asst.professorin Sarada Institute of Science, Technology And Management , Srikakulam, Andhra Pradesh. She received her M.Tech (CSE)from AITAM ,Tekkali,Srikakulam, AndhraPradesh. JNTU Kakinada Andhra Pradesh.Her research areas include Network Security