Journal of Engineering and Applied Sciences 13 (Special Issue 4): 3753-3757, 2018
ISSN: 1816-949X

Cross Layer Security Approach Using Friendly Jammers in Wireless Networks

[1]K. Sivakumar and [2]K.A. Parthasarathy
[1]Department of Computer Science and Engineering,
St. Peter's University, Chennai, India
[2]Department of Computer Science and Engineering,
Akshaya College of Engineering, Kancheepuram, India

Abstract: In wireless networks the security is provided by using the physical layer security that has been recognized as a highly capable design paradigm. The friendly jammers are placed in the access points in order to confuse the signals sent by the eaves droppers. In the proposed technique jamming plays a mean role by creating unwanted signals to baffle the probable eavesdroppers and significantly improves eminence and consistency of secure transportation between legitimate nodes. This jamming signal includes imaginary limits for the exploration of secrecy rate. Particularly, the imaginary limits explore the achievable secrecy rates of user cooperation based jamming whilst the centralized and game theoretic based preceding techniques are reviewed for practical implementations. Jammers should have strong self-interference and the signals.

Key words: Cross layer approach, security, wireless network, friendly jammers, intentional attackers, implementations

INTRODUCTION

Various security risks were introduced in wireless communications due to its broadcast nature as well as the exponential expansion of mobile traffic increases day by day. By using predictable methods of cryptographic mechanisms a secured transportation links are established in the remote transmissions. In recent times to enhance the security, physical layer security method has been renowned as one of the probable solutions in wireless networks by utilizing the characteristics of remote channels. This method is well suited for dynamic networks and distributed processing techniques. Security jamming in physical layer is a good approach to increase the quality of secure wireless transmissions and more jamming signals in addition is required to collapse the eavesdroppers. The jamming signals are created by embedding them with the artificial noise, i.e., intended signal.

The receiver can able to transmit jamming signals by assisting Full Duplex (FD) radios which have the capability to simultaneously transmit and receive the signals. Therefore, FD receiver was exploited to collect the necessary signals while sending jamming signals at the same instant to confound the eavesdroppers. Under all circumstances this transmitting and receiving jamming signals is quite complex due to availability of limited number of antenna. In case of private jammers, they could introduce charges for their dedicated jamming services (Fig. 1).

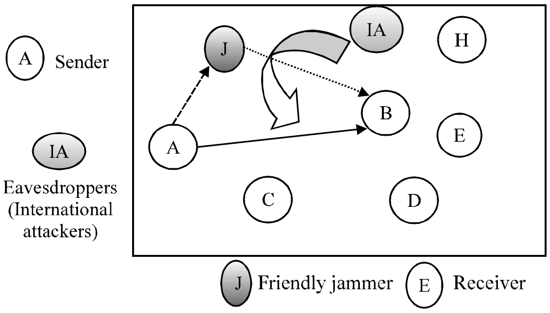

Fig. 1: Network with jammers

This study focuses on physical layer security jamming techniques based on user co-operations and external nodes. Firstly, theoretical limits of jamming through user cooperation are presented and then multi-antenna based jamming techniques are reviewed by exploiting their spatial diversity and Degrees of Freedom (DoF). For example, the advantages of jamming with multi-antenna transmitter can be easily demonstrated by appropriately designing beam-formers such that it would cause a significant interference to the eavesdroppers while no or less interference leakage to the intended receivers. However, the study of theoretical limits of

Corresponding Author: K. Sivakumar, Department of Computer Science and Engineering, St. Peter's University, Chennai, India jamming and the practical designs are necessary to achieve the optimal performance in secrecy networks. This study presents these theoretical limits and design approaches as follows. First, theoretical limits of user cooperation based jamming are explored. Then, centralized and game theoretic based Multiple-Input Multiple-Output (MIMO) transmit and receive pre-coding techniques are discussed to provide efficient jamming services. In addition, Wireless Energy Harvesting (WEH) based jamming techniques are presented through the recent advancement in Simultaneous Wireless Information and Power Transfer (SWIPT) concept. Finally, future research challenges of jamming schemes are briefly discussed.

Literature review: An adversary (intentional attacker) node (Pelechrinis *et al*., 2011) can frequently transmit a data lines in order to chunk any legitimate access happens in the network medium that interferes with the reception of the incoming sequences. This corresponding action refers to 'jamming' and the nodes causes these effects are referred to as 'jammers'.

Jammer Assisted User-Pair Selection (JAUPS) (Lou *et al*., 2015) is a Security-Reliability Tradeoff technique was proposed to provide the physical-layer security in a wireless network. The network consists of various user pairs as well as multiple eavesdroppers (intentional attackers) that are deployed by an opponent manually for trapping the private transmissions that occurs in between the user pairs deliberately. The artificial noise is generated by the friendly jammers that are specially considered onto the illogical space of the main channel for the sake of not intrusive with the target but to collapse the intentional attackers. To evaluate the wireless SRT performance, the friendly jammer on the legitimate user transmissions and eavesdroppers are taken into account self-interfering factor and jamming factor, respectively.

To enhance the secrecy performance the Source-Based Jamming (SBJ) scheme (Lv *et al*., 2017) was proposed for un-trusted relay networks. Here the direct link is employed in secure transmission that provides flexibility cooperation. Also by using this SBJ mechanism the average secrecy capacity is maximized by undertaking the power of the information and jamming signals as well as power of the source and relay nodes.

Detection of pollution attacks and the congested lossy wireless network environment are done using the proposed scheme called efficient cooperative watchdog monitoring method (Li *et al*., 2015). This greatly reduces the overheads of normal transmission modes rather than retransmitting the lost packets and cooperatively shares the packet information among watchdogs. The corrupted packets are detected using randomly generated Vander monde hashes by means of watchdog. This technique has the capability of detecting successive colluded adversaries and achieves low computational complexity. The similar information's are broadcasted to the group of users who have legitimate access in the network using secrecy rate optimization for secure multicasting scheme (Ding *et al*., 2016). Here, the transmitter transmits the information in the presence of eavesdroppers. This scheme is characterized with minimal power and maximum secrecy rate. The jamming services are performed on the basis of benefits thus the jammers charges the transmitter based on the amount of the interference caused to the eavesdroppers.

To overcome the problems faced by the selective jamming attacks Packet-Hiding Methods (PHM) (Pelechrinis *et al*., 2011) was proposed in the network. A difficult opponent node which is aware of network secrets, information details and the implementation details of network protocols at any layer in the network stack can collapse the network entirely. The intentional attacker called adversary has internal knowledge of network for launching selective attacks in which specific messages which are highly importance are targeted. To overcome these attack cryptographic mechanisms with PHY-layer attributes are used. Strong security properties with minimal impact on the network performance can be achieved but creates huge overhead in the network.

Public Key Cryptography (PKC) is introduced in the proposed Authentication framework with Conditional Privacy-preservation and Non-repudiation (ACPN) (Proano and Lazos, 2012) scheme. PKC is applied to the fictitious name production that ensures legitimate third parties to achieve the non-repudiation of vehicles by obtaining vehicles' real IDs. The ID-based signature (IDS) scheme and the ID based Online/Offline Signature (IDOOS) scheme is used for authentication purpose among the nodes, respectively.

In particular, the jammers that are required to attack the wireless network must scale with the BS density (indicates non trivial behavior) only until a certain value beyond which it decreases. Wormhole attack detection algorithms (Ji *et al*., 2015) are used to perceive wormholes and show its precision severely. Scattered Detection Algorithm against Wormhole coding systems (DAWN) investigates the flow directions changes of the innovative envelopes that contain information. DAWN undertakes the good lower bound of victorious recognition rate.

MATERIALS AND METHODS

Cross layer security approach selective jamming attack: Security in physical layer was initially implemented for providing security and to ensure the positive secrecy rate for the transmitted message and the received message. The secrecy rate computational cost is high and in order to reduce the computational cost Cross Layer Security Approach (CLSA) is proposed. The secret key for the data is produced in the physical layer stack and carried out through all the layers of data transmission. Hence, the opponent node cannot inject false information in the middle process. Friendly reactive jammers are placed at the junction point of the network, however, the jammers cannot chunk all the eavesdropper indication, since, the multiple eavesdroppers with unknown location information can attack.

Implementing security is necessary to prevent the data from loss or hacking. Providing security in the physical layer is must, so that, initially generated data will pass over securely. Jamming can be ineffective for many causes like it might miss or act in response too late to a target frame or the jamming signal may lack in signal strength. The friendly jammers are generally power constrained which fixed on access points by legal relations.

Secrecy rate for transmitted and received message: Source node and destination node are fixed, source node generates data according to the destination's requirements and the achievable secrecy rate for this generated message that is transmitted over source node to destination node is measured and this data rate should be entirely hidden from the eavesdroppers. Through this the performance reliability is evaluated in terms of its probability of error while the source node s transmits the message to the destination node at certain secrecy rate R_{sd}:

$$T_s = R_{sd}\left[\log_2(1+\theta\varepsilon)-\log_2(1+\theta e)\right]^{+1} \quad (1)$$

$$R_m = R_{sd}\left[\log_2(1+\theta\varepsilon)-\log_2(1+\theta e)\right]^{+2} \quad (2)$$

The performance reliability is measured in terms of error probability '$\theta\varepsilon$' and 'θe' in both the transmitted signal 'T_s' and the received message 'R_m'. The transmitted messages from source to destination are passed at certain secrecy rate 'R_{sd}'. If the jammer's signal strength is strong enough compared with the eavesdropper signal strength then the achievable secrecy rate for the received signal remains same and good and also can be improved further (i.e., jammer should emit high jamming signal comparing to the eavesdropper signal).

The sender part or source node includes inter-leaver, channel encoder and modulator; receiver block includes channel decoder, de-inter-leaver and de-modulator. The opponent node (intentional attacker) which present in the network can send the interference signal in any of the layers because it knows the internal network pattern or arrangement and it can put effort to research at high transmission speed. It can classify the 'k' number of packets in terms of packet size and necessary redundancy bits are added for security key purpose. The fixed key is used as security key for the packet 'k' and this fixed encrypting key and fixed decrypting key is added for the 'k' packets for both transmitter and receiver. This security measures undertaken in the CLSA initiated with physical layer would be the perceptive solution for the reactive jamming attacks. The 'k' packet can be encrypted by using cipher-text block $C_{i,s}$:

$$C_{i,s} = E_s(C_i \oplus \langle K \rangle_i) \quad i=1, 2, ..., n \quad (3)$$

Where:

E_s = Encrypted key
K_i = Packet

The plain text m can be recovered using the equation:

$$K_i = C_i \oplus D_s(C_{i+1}) \quad i = 1, 2, ..., n \quad (4)$$

where, D_S is decrypted key. To interfere and destroy the normal operation mode the intentional attacker performs packet classification by developing the inter-packet timing information for packet transmissions. The reactive jamming attack by intentional attackers can be prohibited by using the generated secret key using cipher-text cryptanalysis mechanism. The competence of selective reactive jamming of eavesdroppers is reduced by using this cryptanalysis mechanism since the characteristics of packet length and inter-packet timing get changed. However, the signal indication gets distracted randomly.

RESULTS AND DISCUSSION

The proposed scheme CLSA performance is analyzed using the simulation tool Network Simulator-2 (NS2). It is an open source programming language written in C++ and OTCL (Object Oriented Tool Command Language). It is mainly used to model the network protocols and the nodes are distributed in the simulation environment randomly. The parameters used for the simulation are tabulated in Table 1. Transmission Control Protocol (TCP) is the communication protocol used by the nodes to

Table 1: Parameters of packet delivery ratio

Parameters	Values
Nodes in network	50
Routing scheme	AODV
Traffic model	VBR
Simulation area	1000×1000
Channel	Wireless channel
Transmission range	200 mts
Communication protocol	TCP
Antenna	Omni antenna

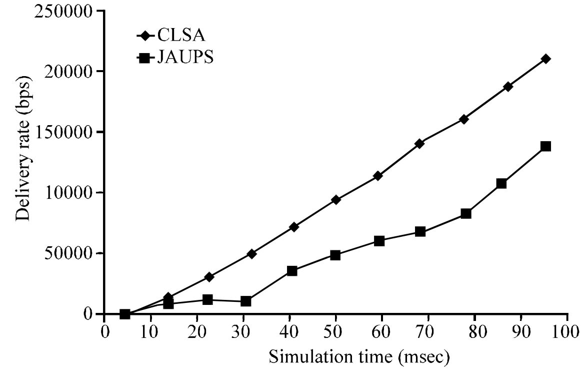

Fig. 2: Packet delivery rate

communicate with each other. Variable Bit Rate (VBR) is used to handle the network traffic. The radio waves are propagated through two-ray ground propagation model, so that, each node in the network receives the signal from all direction by using the Omni directional antenna. The performance of the proposed scheme is evaluated by the parameters packet delivery ratio, packet loss ratio, average delay and throughput.

Packet delivery rate: Packets that are successfully delivered to the receiver is said to be packet delivery rate. Figure 2 shows the PDR of the proposed scheme CLSA. The delivery rate is higher than the existing method of JAUPS. The greater value of PDR means better performance of the protocol.

Packet loss rate: Packet Loss Rate (PLR) can be termed as total number of packets lost during the data transmission. The PLR of the proposed scheme PIIA is lower than the existing scheme PHM in Fig. 3. Lower the PLR indicates the higher performance of the network.

Delay: Delay is defined as the difference between packets received time and the packet sent time. Figure 4 shows that the delay value is for both the existing and the proposed scheme CLSA. The minimum value of delay means that higher value of the throughput of the network.

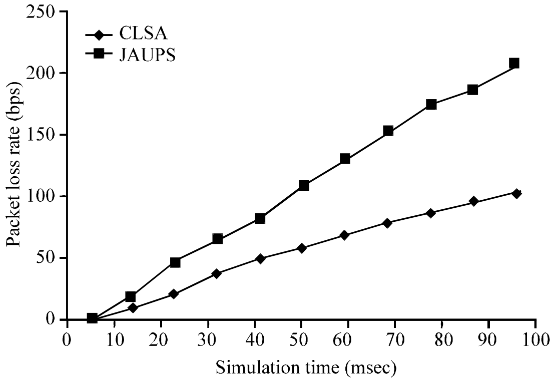

Fig. 3: Packet loss rate

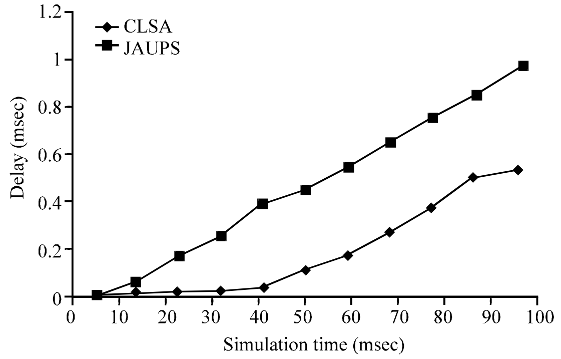

Fig. 4: Delay

CONCLUSION

The friendly jammers are placed in the access points in order to confuse the signals sent by the eaves droppers. In the proposed CLSA technique jamming plays a considerable role by creating unwanted signals to baffle the probable eavesdroppers to avoid the intentional attacks thereby significantly improves eminence and consistency of secure transportation between legitimate nodes. This jamming signal includes imaginary limits for the exploration of secrecy rate. Particularly, the imaginary limits explore the achievable secrecy rates of user cooperation based jamming whilst the centralized and game theoretic based preceding techniques are reviewed for practical implementations. The simulation results are used to verify the advantages of the CLSA scheme.

REFERENCES

Ding, X., T. Song, Y. Zou and X. Chen, 2016. Security-reliability tradeoff for friendly Jammer assisted user-pair selection in the face of multiple eavesdroppers. IEEE. Access, 4: 8386-8393.

Ji, S., T. Chen and S. Zhong, 2015. Wormhole attack detection algorithms in wireless network coding systems. IEEE. Trans. Mobile Comput., 14: 660-674.

Li, J., H. Lu and M. Guizani, 2015. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans. Parallel Distributed Syst., 26: 938-948.

Lou, X., H. Yao, C.W. Tan and J. Wang, 2015. Vander: Efficient cooperative watchdog monitoring for Lossy wireless network coding. IEEE. Trans. Veh. Technol., 64: 702-713.

Lv, L., J. Chen, L. Yang and Y. Kuo, 2017. Improving physical layer security inuntrusted relay networks: Cooperative jamming and power allocation. IET. Commun., 11: 393-399.

Pelechrinis, K., M. Iliofotou and S.V. Krishnamurthy, 2011. Denial of service attacks in wireless networks: The case of jammers. IEEE. Commun. Surv. Tutorials, 13: 245-257.

Proano, A. and L. Lazos, 2012. Packet-hiding methods for preventing selective jamming attacks. IEEE. Trans. Depend. Secure Comput., 9: 101-114.