A Review on Improving the Efficiency of the Network Attack Detection Using Global Inspector

Adarsh D. Mamidpelliwar, Prof S. Kumbhalkar, Prof S. Kuntawar

Abstract— **In wireless transmission the data is transferred by victimization radio signals and it may be overheard by unauthorized user because of broadcast nature of radio propagation. On defend the wireless communication against eavesdropping attacks the physical layer security is raising as a promising paradigm. In recent studies, principally focus is on solely rising the security level like artificial noise generation and beam forming technique, diversity techniques like cooperative diversity, MIMO and multiuser diversity, all such methods Consumes additional power and exhibit high implementation complexity. In this paper, the study relies on simulations by use of 'Global Inspector' as a significant role, that uses the distinctive ID for every node and every packet is passed from source to destination through global Inspector. By victimization GI it's possible to find malicious node, improve the network routing load and also the network communication jitter which defines the efficiency of the system. The network design, challenges and views of the research is additionally addressed during this review.**

Index Terms— **Distinctive ID, Diversity Technique, Eavesdropping Attack, Global Inspector (GI), Network Jitter.**

I. INTRODUCTION

During the past decades, wireless communications infrastructure and services are proliferating with the goal of meeting quickly increasing demands. In line with the newest statistics released by the International Telecommunications Union in 2013, the number of mobile subscribers has reached 6.8 billion worldwide and virtually four-hundredth of the world's population is currently using the internet. Meanwhile, it's been reported in that an increasing range of wireless devices area unit abused for illicit Cyber-criminal activities, as well as malicious attacks, computer hacking, data formation, money information stealing, online bullying/stalking, and so on as in [9]. Hence, it's of dominant importance to boost wireless communications security to fight against cybercriminal activities. In wireless network, transmission of data between legitimate users will easily be overheard by associate eavesdropper for interception because of broadcast nature of the wireless medium. Existing systems generally use cryptographic techniques for preventing eavesdroppers from intercepting data transmissions between legitimate users as in [2],[3], however the protection of a crypto graphical approach would be compromised, if an efficient technique of solving its underlying hard mathematical problem was to be discovered.

Recently, physical-layer security is emerging as a promising means of protecting wireless communications to achieve information-theoretic security against eavesdropping attacks. As in [14] Wyner examined a discrete memory less wiretap channel consisting of a source, a destination as well as an eavesdropper and proved that perfectly secure transmission can be achieved, if the so-called secrecy capacity was developed, which was shown to be equal to the difference between the channel capacity of the main link and that of the wiretap link. The secrecy capacity can be increased by exploiting sophisticated signal processing techniques, such as the artificial-noise-aided security, security oriented beam forming, security-oriented diversity approaches and so on. But, all such methods consume extra power and build issues related with node order dependency therefore the delay related issues.

In this paper, the study is especially supported to reduce the problems related efficiency of the system i.e. Jitter, network routing load and also improving authentication by using global inspector that uses distinctive ID to each node and each packet is passed from supply to destination through GI or global intermediate node (GIN). Also, we'll discuss in details regarding numerous strategies implemented related to this topic and also the methodology that we tend to use to beat the issues.

II. LITERATURE SURVEY

This section describes previously proposed studies for protecting physical layer from eavesdropping attacks and jamming. To improve the credibleness of physical layer, as in [1] paper revealed by Yulong Zou, Jia Zhu has mentioned regarding the many diversity techniques like MIMO, cooperative diversity, multiuser diversity that is employed to enhance secrecy capability of wireless transmission and avoid eavesdropping attacks.

Manuscript received March, 2017.

First Author name**, Dept. Electronics and Communication Engg, Gondwana University, Ballarpur, India, +91 9403875216 **S

***econd Author name**, Dept. Electronics and Communication Engg, Gondwana University. Ballarpur, India, +91 9975116205*

***Third Author name**, Dept. Electronics and Communication Engg, Gondwana University. Ballarpur, India, +91 8983200835.*

As in [4] Hong Xing, Peng Xu describes regarding the theoretical limit and practical design of jamming that generates a noise signal to confuse the potential eavesdropper, for theoretical limits of user cooperative based jamming is employed and for the practical design of MIMO jamming as well as the game theoretic base jamming techniques are mentioned.

A Paper published as in [5] by Pedro C. pinto and Moe Z. Win mentioned regarding techniques for enhancing physical layer security. They proposed two techniques to boost the connectivity of the iS-graph: Sectored transmission and eavesdropper neutralization.

A Paper published as in [7] by Kamel Tourki and Mazen O. Hasna investigate regarding the spectrum sharing incentives to enhance the physical layer security. They form a pair of source and destination, communicating in the presence of passive eavesdropper stimulates the help of another source and destination nodes looking for transmission opportunities, referred to as the secondary network. For that they proposed a cooperative scheme, whereby the secondary transmitter can act as a friendly jammer to confuse the eavesdropper and can share the spectrum to the primary network. All these methods cover the techniques for avoiding eavesdropping attacks, however, according to my survey they didn't concentrate on to raising the energy efficiency, delay or we will say jitter and therefore the network routing load that is we tend to focus on.

III. Proposed Methodology

Proposed work relies on global Inspector or known as global Intermediate node (GIN) that uses distinctive ID or Address to each node that is registered within the GI. When forming a network the packet is passed through GIN from source to destination. Direct sending of data between source to destination is not attainable and hence it improves the authenticity, if any eavesdropper making an attempt to leak data the GIN will check node Id and if that node is not registered within the GIN it will be identified and can be removed as in [13]. The global inspector will check whether the incoming message is eavesdrop by the snooper by checking its source address, If the message is eavesdrop then it will get dropped otherwise global inspector will pass it ahead. At the destination node, it'll be checked if the packet has come from the trusty node i.e. global inspector, if that the packet will be accepted otherwise it'll get dropped.

At present, there are two basic relay protocols: amplify-and-forward (AF) and decode-and-forward (DF). In the AF protocol, a relay node simply amplifies and retransmits its received noisy version of the source signal to the destination. In contrast, the DF protocol requires the relay node to decode its received signal and forward its decoded outcome to the destination node. It is concluded that multiple-relay-assisted source signal transmission consists of two steps: 1. the source node broadcasts its signal with ID. 2. GI nodes retransmit their received signals. The work relies on simulations for that it needs bound algorithm, initially we will define the network options like no. of nodes, routing protocols, directions afterward we'll define Network animation (NAM) file and Trace file. The NAM file can show the network animation for operation and Trace file can show the network trace like sending, receiving and conjointly delay. Awk file is employed for to indicate graph file using the information of trace file then we will configure the node with the network option that we defined. After thta create nodes and place it and begin node communication between source to destination with the help of UDP agent and network agent protocols, once completion of communication it will stop communication so we can run NAM file and it will show the Graph. The figure 1 shows the diagram of network attack detection using global inspector in this source ID and Destination ID is used for authentic communication and data can pass solely from GI and unregistered node cannot make communication among system.

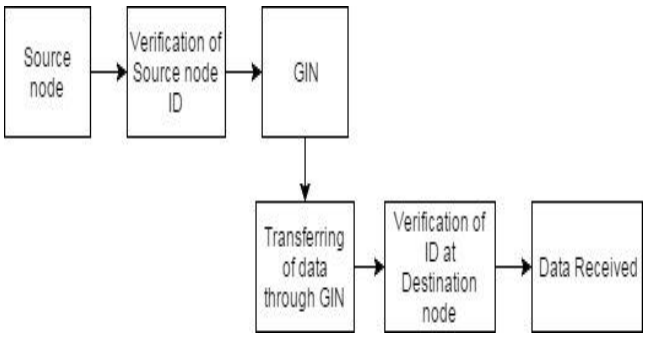

Fig.1 Block diagram of n/w attack detection using global inspector.

Proposed work will be divided into the subsequent modules,

1. Creation of network
2. Deployment of authentic and malicious nodes
3. Development of cooperative communication for node checking
4. Development of Global Intermediate Node for node checking
5. Performance analysis and comparison

This work is independent of node order and has main focus on the authenticity of other nodes via a global Intermediate Node, which acts as a network pass through and helps in authentication and proper communication.

IV. Conclusion

This article studies the physical-layer security of wireless communications and presents several techniques used for improving wireless security against eavesdropping attacks. Specifically, most of the existing work is focused on enhancing the wireless secrecy capacity against the eavesdropping attack only, but they neglected issues like node order dependency and energy efficiency of the system. The proposed work is independent of node order and contains a main focus on the authenticity of different nodes via a global Intermediate Node, that acts as a network pass through and helps in authentication and proper communication. Also it will reduce the delay and improve

efficiency of the system, i.e. jitter, will improve network routing load and can find the malicious node. It can be utilized in several applications like military application for node authentication and mobile network application for checking of node with higher energy efficiency for the network. The proposed work relies on the GI node that is not reliable all the time; however it is easy to implement by comparing other existing methods. Therefore, it's of interest to analyze the reliability, and throughput for the wireless physical layer.

ACKNOWLEDGMENT

This research was supported by publisher of this paper. We thank our colleagues from Ballarpur institute of technology who provided expertise that greatly assisted the research. Also, for sharing their pearls of wisdom with us during the course of this review paper.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and V. Leung, Improving physical-layer security in wireless communications through diversity techniques, IEEE Network, vol. 29, no. 1, pp. 42-48, Jan. 2015.
[2] M. E. Hellman, "An Overview of Public Key Cryptography," IEEE Commun. Mag., vol. 16, no. 6, May 2002, pp. 42–49.
[3] S. V. Kartalopoulos, "A Primer on Cryptography in Communications," IEEE Commun. Mag., vol. 20, no. 4, Apr. 2006, pp. 146–51.
[4] Hong Xing, Peng Xu, "Physical Layer Security Jamming: Theoretical Limits and Practical Designs in Wireless Networks," IEEE Access, vol. pp, no. 99, Dec. 2016, pp. 1-1.
[5] Pinto, P.C., J. Barros, and M.Z. Win. "Techniques for Enhanced Physical-Layer Security." GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference. 2010. 1-5.
[6] T. Akitaya, S. Asano, and T. Saba, "Time-domain Artificial Noise Generation Technique Using Time-domain and Frequency-domain Processing for Physical Layer Security in MIMO-OFDM Systems," IEEE Int. Conf. Communications (ICC), pp. 807 – 812, June 2014.
[7] K. Tourki and M. O. Hasna, "Proactive spectrum sharing incentive for physical layer security enhancement," in Proc. IEEE Global Commun. Conf., pp. 1-6, Dec. 2015.
[8] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", CACM, Vol. 47, No. 6, June 2004.
[9] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," Appear to: Proceedings of the IEEE, 2016.
[10] A. Nosratinia, T.E. Hunter, and A. Hedayat, "Cooperative Communication in Wireless Networks," IEEE Comm. Magazine, vol. 42,no. 10, pp. 74-80,Oct. 2004.
[11] V. Raghunathan. C. Schurgers, S. Park, and M. B. Srivastava. Energy aware wireless microsensor networks. IEEE Signal Pmcessing Magozine, vol. 19. iss. 2. pp. 40-50. March 2002.
[12] K. C. Chan and S. H. G. Chan, "Key management approaches to offer data confidentiality for secure multicast," IEEE Network Mag., vol. 17, no. 5, pp. 30–39, Sep. 2003.
[13] M. Ali and Z. A. Uzmi. An energy-efficient node address naming scheme for wireless sensor networks. In IEEE INCC'04.
[14]A. D.Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.
[15] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in Proc. of 46th Annual Allerton Conference Commuication, Control, and Computing, pp.1132–1138, Sep.2008.