International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Routing Methodology for Secure Transmission of data in Physical Layer

S.Vandana, T.Madhavi

Abstract: ***The difficulties of privacy and security in WANETs have taken on a step by step more vital responsibility as those networks persist to increase their role globally. Historically, physical layer is regarded as biased function addressed below the security, and all broadly used cryptographic protocols like Rivest-Shamir–adlemen, Advanced encryption standard and Data Encryption standard are developed and applied assuming an error-free physical layer already exists . Contrasting the traditional cryptography which neglects distinction among the communication channels, the current physical layer safety accomplish data protection using well designing channel code consistent with the channel capacities assuming that the authentic data can never be recovered.***

The standard system protection makes use of encryption and deciphering activities inside the application layer. Under any circumstances, this won't just construct the computational overhead of system. There's no actual way to avoid eavesdropper listening in and assault from the physical layer. Addressing this problem, this paper proposes a basic system model in which the cooperative relay broadcast channel with the user cooperation is introduced and the overall performance metrics based on the physical layer safety can viably enhance the system protection limit.

Key Words: WANETs, Cryptography, Eavesdropper.

I.INTRODUCTION

Security in WANETs is viewed as a significant issue , in light of its communicate nature, as remote multiuser correspondence is incredibly at risk to listening quietly by eavesdropper, it is necessary to maintain the communicated data secure. The increase of dynamic and large-scale systems compels novel problems on traditional safety efforts like network layer cryptography. In this regard, misusing the physical layer is considered as a substitute to attain great mystery without requiring key distribution and complex encryption/decryption algorithms. With the recent advancements in technology, the security of physical layer is measured as dynamic research area and was evidenced vital development. Broad research endeavors have been dedicated to be familiar with the exhibition of physical layer security. At first the highest secure data rate in discrete memory less wire-tap channel, where the transmitter, legitimate receiver and unauthorized receiver are concerned and the existence of channel codes to make sure the message is delivered to legitimate receiver forever while ensured at unauthorized user is examined [1]. This attempt was then extended to Gaussian wire tap channel in which reliable transmission is achieved if wire-tap channel is superior to main channel [2],Rayleigh fading wire-tap channel in which

data was securely transferred in presence of a unauthorized receiver from legitimate transmitter to a legitimate receiver [3],confidential messages transfer in broadcast channels with secret messages [4]. In light of these revolutionary efforts on the fundamental point-to-point wire-tap channel, numerous ongoing exploration endeavors have been performed to comprehend the exhibitions of physical layer security in large scale remote specially appointed systems, in which several authorized nodes and eavesdroppers are included.

B. D. V. Veen instigate beam forming as a versatile type of spatial filtering. Functions carried out in block adaptation and information are predictable commencing a data array of sequential block with constant adaptation and the loads are changed as for the inspected information. The fundamental versatile calculations are two which presented as Least Mean Squares and Normalized Least Mean Squares. The paper features partial adaptivity, however it didn't addresses signal cancellation issues [5].

In the article author Chen, X. and Lei, L expressed the personal and mobile communication service, for example, utilizing of wireless communication applications is developing quickly. They proposed the utilization of adaptive or smart antenna arrays using spatial spectral method for an augmentation in the channel capacity. The smart or adaptive array exhibit signal range just as and nature of mobile phone clients might be expanded with tracking facility. The third generation wireless systems in the telecommunication sector in which the quality, range and tracking region of smart or adaptive antenna system has a wide importance. The 3G frameworks utilizing smart antenna or adaptive issues are handled viably yet multi antenna eavesdropping is disregarded [6].

Weng defined the broadcast communication capability of a wireless network using common fading of desired signal and intrusive signals. The effect of unauthorized user on the broadcast transmission capacity of a wireless network with secrecy outage constraint is also characterized. Results demonstrate performance restrictions of a network synchronized with another heterogeneous networks and trade-offs between various system parameters, and thus suggest network design of protocols which require local broadcasting in distributed network optimization [7].

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
S.Vandana*, Assistant Professor, Electronics and Instrumentation Department, VNR VIGNANA JYOTHI Institute of Engineering And Technology at Hyderabad
T.Madhavi, Professor, Electronics and Communication, Department in GITAM Institute of Engineering And Technology at Vishakapatnam.

To provide WANETs with secure communication, several researchers attempted dissimilar methods to generate the session keys. Guo proposed a cluster-based safe transmission mechanism in WANETs. A multi-agent system with several intelligent agents are scattered in the network. The plan applies the D-H key switch procedure for the session key establishment. It assists the cluster head to decrease the transmission burden, to keep away f the time synchronization difficulty in nodes authentication and to preserve the entire privacy requirements [8].

Yang focuses on a multi-hop WANET with two distinctive broadcast schemes amplify-and-forward and decode and-forward , and search the route selection through consideration of security and QoS together. Depending on both the schemes, a route metric is formulated which enable us to choose the appropriate route and a flexible route selection algorithm is proposed for message delivery depending on diverse security and QoS needs [9].

WANG Yajun in his paper investigated the transmission scheduling for a wireless Adhoc network involving various source-destination pairs within the sight of a eavesdropper. An ideal transmission scheduling scheme for securing the adhoc network against eaves- dropping, where a source-destination pair with the most elevated secrecy rate is scheduled to access their shared wireless mechanism for information transmission is proposed. The regular round-robin one of the cooperative transmissions scheduling approach was as well considered as a benchmark, in which the different source-destination pairs alternate in getting to the wireless medium. He determined closed form secrecy outage expressions of both the round-robin transmission scheduling and the planned optimal transmission scheduling schemes in Rayleigh fading conditions. Numerical outcomes demonstrated that the proposed transmission scheduling performs superior to conventional round-robin scheduling in terms of its secrecy outage probability. At long last, after expanding the quantity of source-destination pairs, the secrecy outage probability of the proposed ideal transmission scheduling scheme improves altogether, unequivocally indicating the security advantages of misusing the transmission scheduling against eavesdropping attacks[10].

Ian and Elizabeth in their paper describe the event triggers required for AODV operation. They created AODV- UCSB implementation and validated the AODV routing protocol design using the implementation [11].

The main objective of our work is to propose a solution to challenges regarding security in the network systems while transferring the data from source to destination .Since conventional techniques are lacking in protection aspects, a routing protocol in which data was securely transferred was proposed .The aim is to study the proposed scheme and compare with traditional algorithm the performance metrics.

II. IMPLEMENTATION

The existing work is selected such that the data transmission from source to destination has to be done securely through Routing in any network; it be wired or wireless. Routing is the method of selecting the path for transfer of information from a source to a destination. Data transmission between transmitter and receiver should be inside the communication range of the antenna. If direct transmission is chosen there will not be any intermediate nodes existing in between the transmitter and receiver for sharing of data.

The compound multiple access channel is utilized by the relay-eavesdropper channel, where transmitter/relay to receiver is considered as the initial mac and transmitter/relay to hearer is selected as the afterward. R1 is the codeword rate of the transmitter, and R2 is the codeword rate of the relay. If the relay doesn't broadcast, the right secrecy rate is zero for the input distribution since R1(A)<R1(B).Further, if the transmitter and the relay synchronize their communications, an equivocation rate (Re) is achieved which is strictly greater than zero. A positive perfect secrecy rate can still be preserved in the non existence of relay by working at point A. By moving to the operating point B, it is probable to get a higher secrecy rate. It is a multi relay transmission which gives more secure connection but not viable when eavesdropper attacks.

So a basic cooperative relay broadcast channel model in which effects of user cooperation on the secrecy of broadcast channels is introduced in this paper. An achievable scheme that combines coding scheme for broadcast channels and also cover the relay channel is proposed. To obtain positive secrecy rates for both of the users, different assignment for auxiliary random variables appearing with achievable rate is provided. This auxiliary random variable assignments combining with relaying to provide secrecy for both users when the relaying user is weak.

AODV obtains the routes purely on-demand which makes it a very useful and desired algorithm for WANETs. The reactive on demand routing protocols set up the route to a specific destination just on the off chance that it is required. Adhoc on-request Distance Vector (AODV) is one of the ordinarily utilized reactive on demand routing protocols in wireless ad hoc network. Every single intermediate node of the road hub that takes an interest in handing-off this answer to the source hub makes a forward route to destination. Before the establishment of connection between the source and destination, the routing protocol ought to be referenced to establish the connection between them.

The performance of different WANET routing protocols was measured by a number of quantitative metrics. RFC2501 illustrates metrics that can be used for evaluation. To analyze whether data was securely transmitted between source and destination, three performance metrics Throughput, Delay and Packet loss are evaluated

III.SIMULATION RESULTS AND ANALYSIS

The performance of the routing methodology was measured with the help of network simulator NS2. The topology comprises of 35 nodes in a 500m × 500m grid. The communication range used is 100 m. The number of nodes considered is 35. Throughput, measuring the packet loss at the receiver and average delay are the primary metrics of interest. The transmitter and receiver are chosen at random. AODV is utilized as the routing protocol.

Every transmitter produces traffic at an extremely high rate to stay back-logged for the complete simulation duration. The simulations are run for 60 s with variable step size.AODV is used for simulation at the network layer and flat-grid topology is introduced . Nodes send constant bit rate (CBR) traffic at varying rates. The following are the parameters used while simulating the performance metrics.

The results after simulation are viewed in the below figures. The performance of routing protocols based on the evaluation parameters Packet Loss, Average Delay and Through put are studied

Parameter	Value
Simulation Tool	NS-2.34
Operating System	Ubuntu 12.04
MAC/PHY layer	IEEE 802.11
Antenna model	Omni directional
Interface queue size	200 packets
MAC	Mac/802_11
Propagation model	Two Ray Ground
Examined protocol	AODV
Interface Queue Type	Queue/DropTail/PriQueue
Mobility model	Random way point
Link Layer Type	LL
Channel Type	Wireless Channel
Topography Dimension	500 x 500
Number of nodes	35

Throughput:

Throughput is the proportion of the total amount of data that is transmitted from the source to destination to the time taken for the last packet of the data to reach the receiver. It measures of effectiveness of a routing protocol. Based on the simulation results, shown in Fig1. The throughput value of existing method gradually increases in the beginning but does not maintain its value when the time increases. The throughput value of proposed method increases at lower pause time and maintain its value as the time increases. Hence, the introduction of cooperative relay broadcasting shows better performance with respect to throughput.

$$\text{Throughput} = \frac{(Received\ data * 8)}{Data\ \ transmission\ \ period}$$

Packet Loss:

Packet loss measures the loss rate of the data from transmitter to receiver it characterizes both the exactness and accuracy of ad hoc routing protocols. The packet loss of existing method is less when compared to other protocols but from the simulation result in Fig2. it was clear that the proposed method has less packet loss when compared with existing method.

$$\text{PacketLoss} = (\text{Generated Packets} - \text{Received Packets})$$

Average Delay:

The Average delay is a measure of how long it takes for packet to reach from transmitter to receiver and represents the reliability of the routing protocol .Even though the AODV does not have lower average delay, the proposed method shows a lower average delay throughout the simulation as shown in Fig3.

delay[j] = receiving_time[j] – sending_time[j]

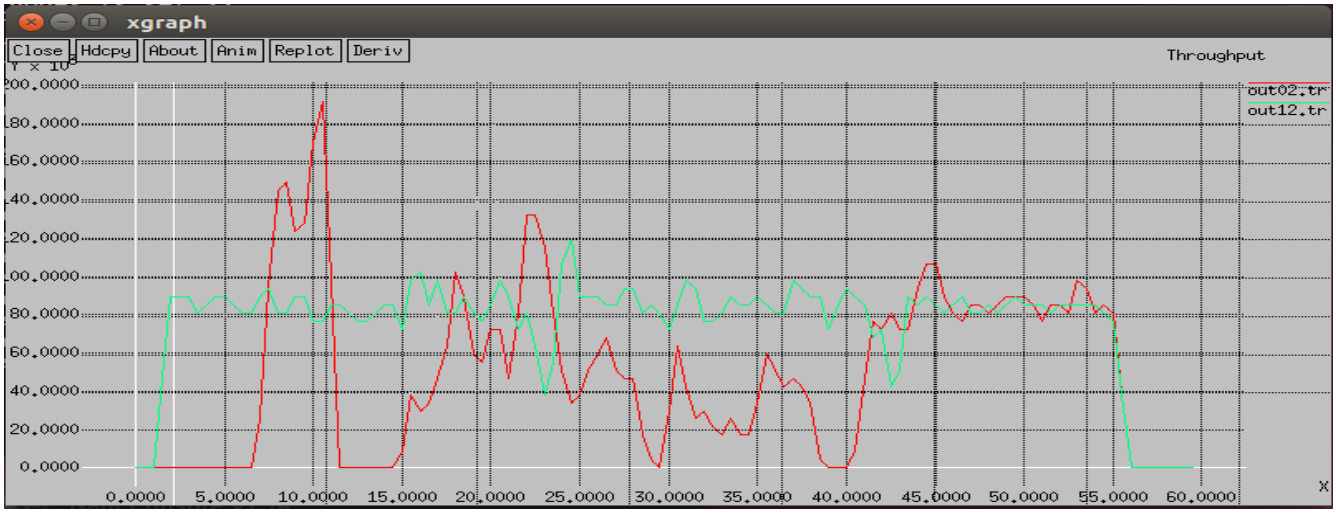

Fig1.Throughput comparison between ExistingMethod and Proposed method

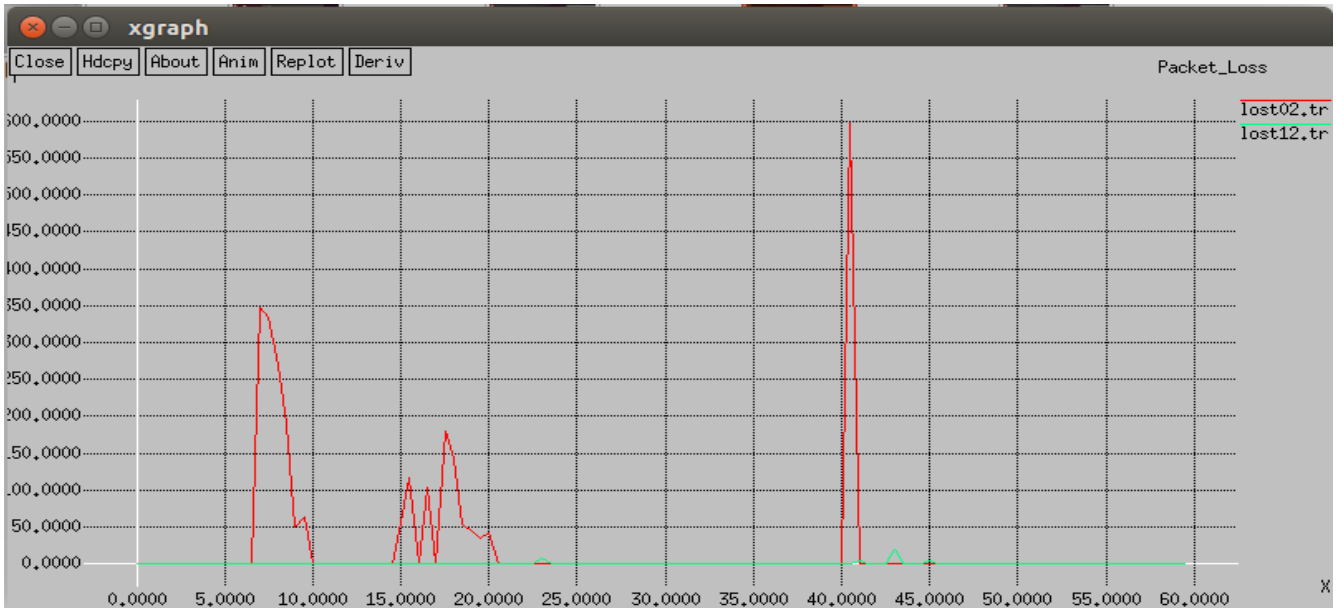

Fig2.PacketLoss comparison between Existing Method and Proposed method.

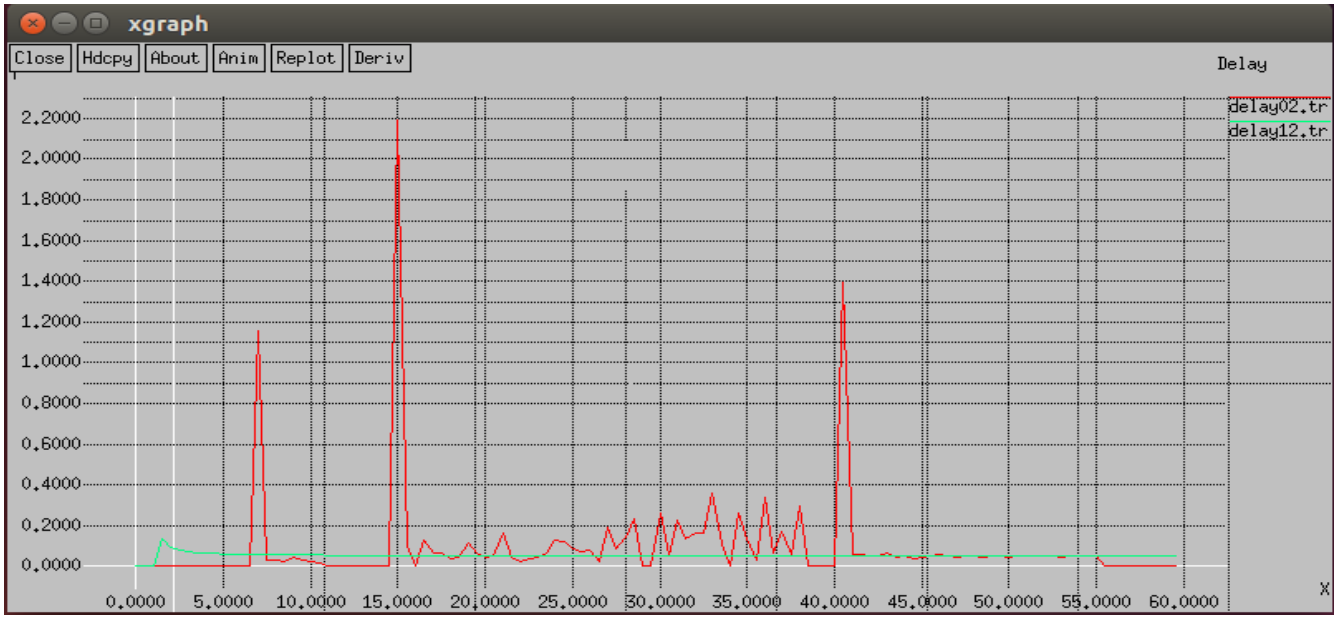

Fig3.Delay comparison between Existing Method and Proposed method

IV.CONCLUSION

This comparison has given overview of the routing methodology of physical layer security in remote systems in light of data theoretic standards. The advancement of secure transmission from transmitter to receiver is depicted. It was proved that the cooperative relay broadcasting with user cooperation shows better performance than compound media access control. Performance parameters throughput, packet loss and average delay are evaluated through the simulations. Different studies show that there won't be any protocol which will depicts better result in all the performance aspects. Hence proposed method improves the performance in terms of packet loss and average delay effectively.

REFERENCES

1. A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975)1355–1387.
2. Jinxiao Zhu Yin Chen , Yulong Shen , Osamu Takahashi , Xiaohong Jiang , Norio Shiratori,Secrecy transmission capacity in noisy wireless ad hoc networks, Science direct, Ad Hoc Networks 21 (2014) 123–133.
3. S.K. Leung-Yan-Cheong, M.E. Hellman, The Gaussian wire-tap channel, IEEE Trans. Inf. Theory 24 (4) (1978) 451–456.
4. M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security, IEEE Trans. Inf. Theory 54 (6) (2008)2515–2534.
5. Van Veen, B.D. and Buckley, K.M., 1988. Beamforming: A versatile approach to spatial filtering. IEEE assp magazine, 5(2), pp.4-24.
6. Chen, X. and Lei, L., 2013. Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee. IEEE Communications Letters, 17(4), pp.637-640.
7. W. C. Ao and K. C. Chen, "Broadcast transmission capacity of heterogeneous wireless ad hoc networks with secrecy outage constraints," GLOBECOM - IEEE Glob. Telecommun. Conf., pp. 0–4, 2011.
8. M.-H. Guo, H.-T. Liaw, D.-J. Deng, and H.-C. Chao, "Cluster-based secure communication mechanism in wireless ad hoc networks," IET Inf. Secur., vol. 4, no. 4, p. 352, 2010.
9. Y. Xu, J. Liu, Y. Shen, X. Jiang, and T. Taleb, "Security/QoS-aware route selection in multi-hop wireless ad hoc networks," 2016 IEEE Int. Conf. Commun., pp. 1–6, 2016.
10. W. Yajun et al., "An Anti-Eavesdrop Transmissionscheduling scheme based on maximizing secrecy outage probability in Wireless ad hoc Networks.China Communications.Jan 2016
11. Chakeres, Ian, Belding, Elizabeth,2004/01/01,"AODV Routing Protocol Implementation Design."Proceedings of the 24th International Conference on Distributed Computingsystems Workshops,Pg: 698-703
12. Van Veen, B.D. and Buckley, K.M., 1988. Beamforming: A versatile approach to spatial filtering. IEEE assp magazine, 5(2), pp.4-24.
13. Godara, L.C., 1997. Application of antenna arrays to mobile communications. II. Beam-forming and direction-of-arrival considerations. Proceedings of the IEEE, 85(8), pp.1195-1245.
14. Litva, J. and Lo, T.K., 1996. Digital beamforming in wireless communications. Artech House, Inc..
15. Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J. and Di Renzo, M., 2015. Safeguarding 5G wireless communication networks using physical layer security. IEEE Communications Magazine, 53(4), pp.20-27.
16. Mukherjee, A., Fakoorian, S.A.A., Huang, J. and Swindlehurst, A.L., 2014. Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys & Tutorials, 16(3), pp.1550-1573.
17. Chen, X. and Lei, L., 2013. Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee. IEEE Communications Letters, 17(4), pp.637-640.
18. Godara, L.C., 1997. Applications of antenna arrays to mobile communications. I. Performance improvement, feasibility, and system considerations. Proceedings of the IEEE, 85(7), pp.1031-1060.
19. Wen-gang, Z., Jing, L. and Hui-ling, G., 2016. The Physical Layer Security Beamforming Method based on Large-scale Multi-antenna. International Journal of Future Generation Communication and Networking, 9(7), pp.307-316.
20. S.Corson and J.Macker, "Routing Protocol Performance Issues and Evaluation considerations", RFC2501, IETF Network Working Group, January 1999.

AUTHOR'S PROFILE

S.Vandana did her Bachelors degree in Electronics and Instrumentation Engineering from Sir C.R.Reddy Engineering College, Eluru and obtained her Masters degree in Embedded Systems from Sri Vasavi Engineering College, Tadepalligudem. She has 10 years of teaching experience and presently working as an Assistant Professor in Electronics and Instrumentation Department in VNR VIGNANA JYOTHI Institute of Engineering And Technology at Hyderabad. Her areas of research include Wireless Adhoc Networks and Embedded Systems. She is a life time member in ISOI and she had publications in various International Journals.

Dr.T.Madhavi did her Bachelors degree in Electronics and Communication Engineering . She has 20 years of teaching experience and presently working as an Professor in Electronics and Communication Department in GITAM Institute of Engineering And Technology at Vishakapatnam. Her areas of research include Wireless Adhoc Networks and Embedded Systems. She had publications in various national and International Journals