IMPLEMENTATION OF OPINION TRUST ALGORITHM FOR SECURE DATA TRANSMISSION IN WANETS

S.Vandana

Assistant Professor, Department of Electronics and Instrumentation Engineering,
VNR Vignana Jyothi Institute of Engineering and Technology
Hyderabad,Telangana,India.
vandanahasini@gmail.com

Dr.T.Madhavi

Professor,Head of the Department, Department of Electrical,Electronics and Communication Engineering,
GITAM School of Technology
Hyderabad,Telangana,India
mtatinen@gitam.edu

Abstract

The increasing rate of users and network capacity creates a necessity to address the challenges in Wireless Ad-hoc Networks. Secrecy of information in wireless ad hoc networks also plays a vital role. Physical layer security is an essential technology to achieve secure information transmission in Wireless Ad hoc networks. Several algorithms are developed to transfer the data between legitimate users with zero information to the eavesdropper appearing with uniform distribution only. In this paper, Opinion Trust Algorithm was developed to improve the transmission rate in Wireless Ad hoc networks considering eavesdropper appearing with uniform distribution as well as random distribution. The performance metrics throughput, packet loss and delay are improved even considering random distribution.

***Keywords*: Eavesdropper; Opinion Trust Algorithm; Random distribution.**

1. Introduction

Information security in WANET's plays an important role because of its broadcast nature. The principle behind secure data communication is to transfer the confidential data between legitimate users while making the unauthorized user (eavesdropper) ignorant of data. In recent years, physical layer security is gaining predominance because it can avoid eavesdropping of the information without assist from upper layers. This feature made the theoretic research on physical layer security become a potential technique in improving information security.

Many researchers have done predominant work on several issues in physical layer security. As opposed to the conventional cryptographic methodologies, there is a promising direction toward accomplishing secure connection through physical-layer security [1]. Data transmission is done between one transmitter and an authorized receiver and an eavesdropper in a free –space optical (FSO) link. The analysis allows us to estimate performance metrics depending on channel statistics. Secure data transmission on a multi –layered architecture is provided by combining physical security and algorithmic security [2].

Anti-jamming scheme was proposed first in which interference was aligned with jamming signal among users. Later, artificial noise was introduced without interference in an authorized network where eavesdropping is disturbed by artificial noise. An eavesdropping scheme with aggressive IA users is also developed to breakdown the potential threat [3]. Providing security for wireless communications is a challenge because of inevitable nature of wireless radio spectrum. A symmetric encryption key is aimed by a secret key generation in physical layer which yields complete secrecy with zero information to the eavesdropper [4].

Physical layer security was considered as a novel approach to reduce the security issues while transferring sensitive data through wireless networks. Conceptual studies have proved its viability to increase the security of wireless communications. Jammer placement algorithms minimizing the number of jammers are introduced [5]. In a multi-user MIMO system, a novel non-linear pre-coder was introduced to enhance the security with multiple eavesdroppers. Adding artificial noise to data before transmitting it will improve the secrecy rate in a physical layer. Bit error rate and secrecy-rate performance was improved by this non-linear pre-coder when compared with the existing work [6].

Two- way relaying for energy efficient secure communication is used to avoid relays from transferring the secret data among users. Optimization algorithm is used to solve the sub problems derived from a complex problem. The developed scheme can enhance the energy efficiency predominantly, which disclose the inbuilt comparison of security and energy [7]. The usage of mobile relaying in increasing secure communication is introduced in this paper. A four-node channel set up with transmit optimization which maximizes the secrecy rate and outperform the static relaying scheme is introduced [8].

OFDM transmission becomes more secure and random using subcarrier obfuscation in physical layer employing OFDM. Search space key rate of the proposed scheme offers better performance when compared with other OFDM encryption algorithms. In this scheme the security level and key rate can be modified because of its uncomplicated nature which is apt for resource constrained devices [9].In order to enhance the secure performance of a physical layer in a cellular network a novel cooperative jamming mechanism was developed [10]. A full-duplex base station with multiple uplinks and downlinks of a cellular network was assigned with a resource block for each uplink and down link.

In an OCDMA system, the security level in a physical layer is measured. The reliability and security of the coherent OCDMA system are computed keeping in view the authorized bit error rate and leakage factor. The increase in code length will enhance the performance of optical code division multiple access system [11].A multi-beam satellite communication system where unauthorized user surrounds authorized user is developed in which achievable secrecy rate is maximized by an optimization problem while maintaining transmit power constraint. Two algorithms are proposed in which the validity of SLNR beam forming algorithm was proved [12].

A communication system with half-duplex relay and an eavesdropper using interference alignment is designed [13] for a physical layer security system. In this algorithm, the user will combine data signals with jamming signals and transmit them through the relay as broadcast. The intended receiver can eliminate the jamming signal maintaining the minimum power requirement where the eavesdropper cannot eliminate the jamming. An encryption algorithm from a multiple chaos generator with time selective channel which produces secret code was designed [14].The encrypted data from the proposed algorithm was successfully recovered by legitimate receiver where the eavesdropper was not able to recover the data.

Relay based cognitive radio network that uses OFDM as the medium access technique for improving physical layer security was proposed. In relay aided CRNs, secure resource allocation has become a difficulty. A relay network which has two dedicated relay nodes was introduced in which power allocation and sub-carrier mapping were optimized maintaining maximum secrecy rate of the CRN [15].A transmission algorithm in a physical layer system which prefers superior channel quality subcarriers for half of the data transfer and XOR of two halves of data bits through the remaining inferior channel quality subcarriers. Perfect secrecy with optimal utilization of system is achieved in this algorithm [16].

A fixed –point digital chaos algorithm improving security in OFDM network with a low computational precision is designed. A fixed-point chaos generating a periodic key streams was used to encrypt the downstream data. High security was attained with low implementation complexity was achieved using the proposed scheme [17]. A novel work improving physical layer security in passive optical networks is of great importance. DH key exchange protocol is employed to provide secure communication. The computational time is decreased by applying Encryption on partial data of I/Q channel [18].

Transmit antenna selection in massive MIMO channels was studied [19]. A subset of antennas was selected to transmit messages from transmitter to receiver. To enhance the secure transmission between transmitter and receiver, a branch-and-bound algorithm was proposed for antenna selection in independent and identical distributed Rayleigh flat fading channel. UAV Communication is foreseen to be broadly applied in the prospective 5G wireless networks, because of its several advantages. Because of the broadcast nature of the wireless channels, secured UAV communication between the desired nodes is required. High mobility of the Unmanned aerial vehicle is used to establish the connection between authorized and degrade the connection for unauthorized. Iterative algorithms are used to establish secure communication between U2G and G2U [20].

A hybrid beam-forming algorithm is proposed in multiple input multiple output mm-wave relay system. In relay communications, the complexity and feedback were reduced in the proposed algorithm. The artificial noise is introduced to fight against the unauthorized. A balance is achieved, and the performance was enhanced through the implementation of the algorithm [21]. The work done so far using Interference alignment, four node channel setup and adding artificial noise and considering the eavesdropper appearing at uniform distribution are proved to have limited performance. By analyzing different problems associated with secure transmission of data, a need for efficient algorithm which transfers the data securely arises. So, in this paper an Opinion Trust Algorithm which considers both the uniform and random distribution of eavesdropper was proposed.

2. System Model

The compound MAC channel is considered as the existing method and the implementation of this method is compared with the Opinion Trust Algorithm. The operation of the compound MAC is as follows. The relay and eavesdropper channel into a compound MAC, in which initial MAC is in between source/relay and receiver and the second one is in between source/relay and eavesdropper. R1 is the codeword rate of the source, and R2 is the codeword rate of the relay. If the relay node does not transmit, the perfect secrecy rate is zero for the input distribution since R1(A) < R1(B). On the other hand, if the relay and the source coordinate their transmissions, equivocation rate (Re) is achieved which is strictly greater than zero. In the absence of relay, operating at point A can still maintain a positive total secrecy rate. More confidentiality can be achieved by switching the operating point to B. It is a multi-relay transmission that gives the connection more secure but not viable when eavesdropper attacks.

The block diagram of an Opinion Trust Algorithm (OTA) system model is as shown in Fig. 1. to enhance the transmission rate in WANETs considering the malicious node. This work aims primarily at transferring of data between two legitimate users securely without eavesdropping. To implement this, a system model using Opinion Trust Algorithm was developed. Firstly, the system node parameters are defined in this model with a total of 35 nodes. Among the 35 nodes, 30 nodes are legitimate nodes and 5 are defined as malicious nodes. The behavior of the malicious node in the system model is to deny service to other nodes in the network and it also modifies data before, during and after transmission. A malicious node alters the entire or a few of the data packets that is made-up to forward. It can also modify the data it produces to defend it from being recognized. In previous malicious detection techniques, malicious node is randomly chosen based on the number of packets dropped. So, sometime legitimate user also treated as the intruders or attacker. It will result into high false positive rate, and it violates the security of wireless networks. Secondly, a network was formed considering all the nodes for data transmission.

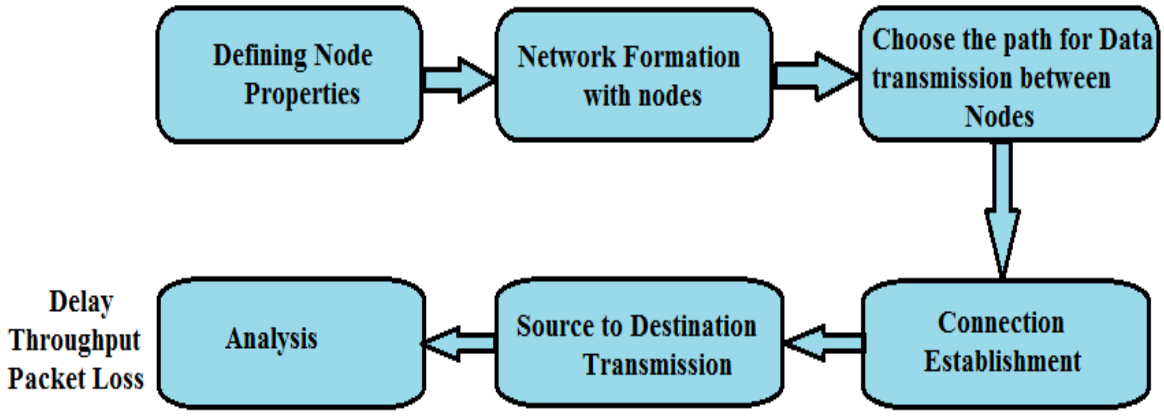

Fig. 1. Block Diagram of System Model of Opinion Trust Algorithm

In this model, the path was established between the nodes by using the Opinion Trust Algorithm and finding the best route for connection establishment. The malicious nodes are detected based on the trust values of the nodes. Constant bit rate service category is used for connections that transport traffic at a constant bit rate, where there is integrated time synchronization between source and destination. All the nodes will have zero trust value at the beginning. If a node is not contributing to packet drop, the trust value of a node will be incremented by 1. The node will be treated as a legitimate node when a particular node reaches its trust value equal to or more than threshold value and is used for further communication.

Each node's trust value is determined and compared with its threshold value. If trust value is not reaching threshold value, then it will be considered as malicious node and it will not be used for further communication. Low false positive rates produced by reducing the packet drop ratio will eventually improve security of WLAN. After determining which nodes are legitimate and which are malicious, a connection was established between source and destination using the legitimate nodes and secure data transmission occurs. Once the data was transmitted, the QoS parameters delay, throughput and packet loss are measured.

3. Simulation and Analysis

The algorithm was implemented using NS2 network simulator. The topology consists of 500m × 500m grid with 35 nodes. The receiver and transmitter are randomly selected for the communication range 100 m. The routing protocol used is AODV. The simulation with variable step size will run for 60 seconds. The different node properties used in the simulation are shown in Table 1.

Parameter	Value
Simulator	NS-2
Version	NS 2.35
Number of Nodes	35
Topography Dimension	500m*500m
Traffic Type	Constant Bit Rate
Signal Propagation Model	Two Ray Ground model
Type of Antenna	Omni directional
MAC Type	802.11 MAC Layer
Routing Protocol	AODV
Interface Queue	Drop Tail / Priority Queue
Maximum Packets in IF queue	200
Packet Size	512
Channel	Wireless

Table 1. Node Properties

The flowchart for the Opinion Trust Algorithm is as shown in Fig. 3. Firstly, the values of trust node and threshold value are initialized with 0 and 100 respectively and assumed one trust value when ten packets are dropped. Trust value will be incremented if packets are correctly transmitted, and if it reaches the threshold value of 100, then that node is considered as a legitimate node. If packets are dropped, trust value will be decremented. If the attained trust value after decrementing is less than the threshold value, then the node will be considered as malicious node.

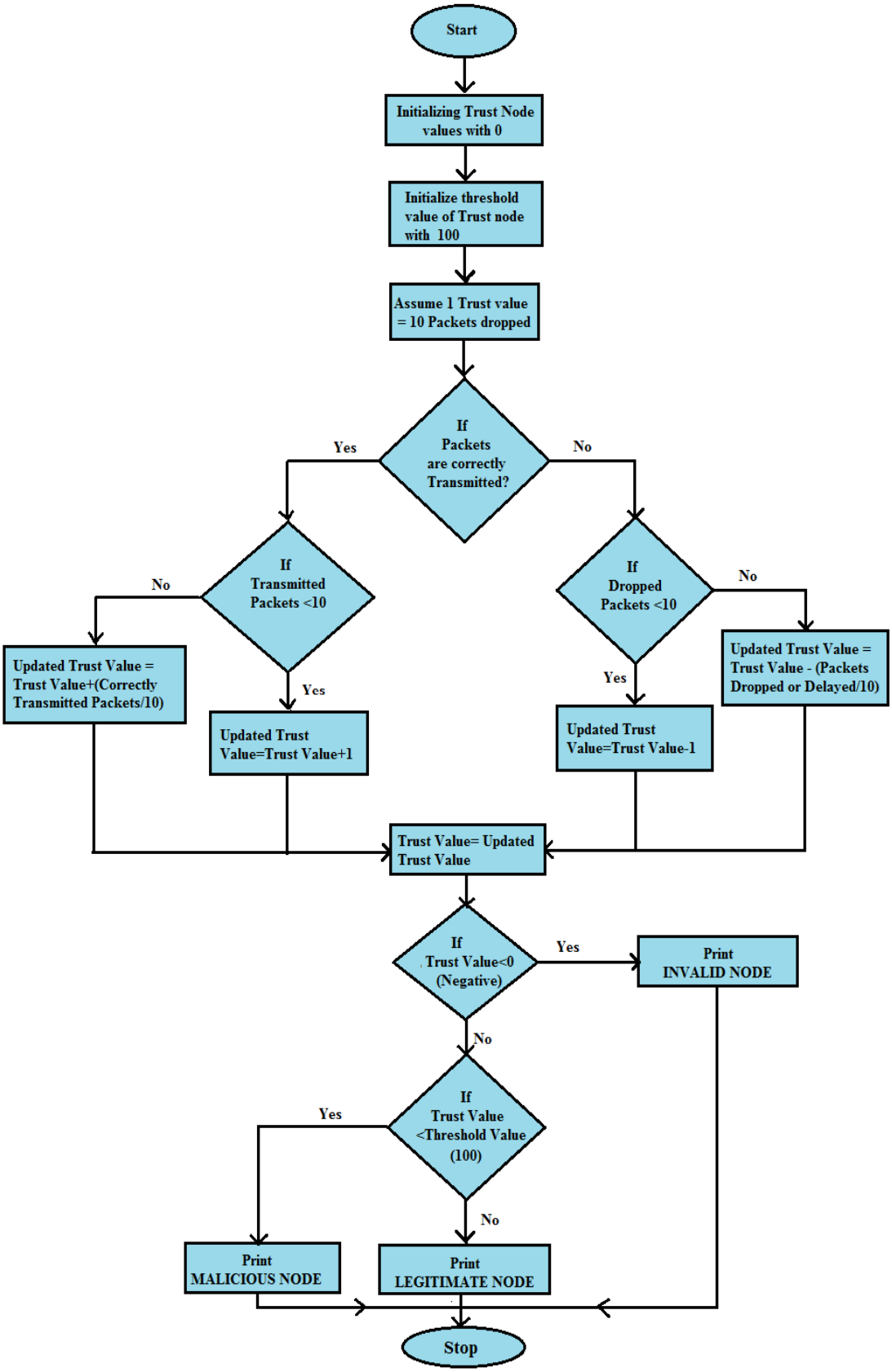

Fig. 2. Flow Chart for Opinion Trust Algorithm

The simulation model with 35 nodes was shown in Fig. 3.The AODV Routing protocol with routing algorithm which chooses the nodes for data transmission is as shown in Fig. 4.The Request to send, Clear to send, Data packets, Acknowledgement and Packet Drop are shown in Fig. 5. to Fig. 9. respectively.

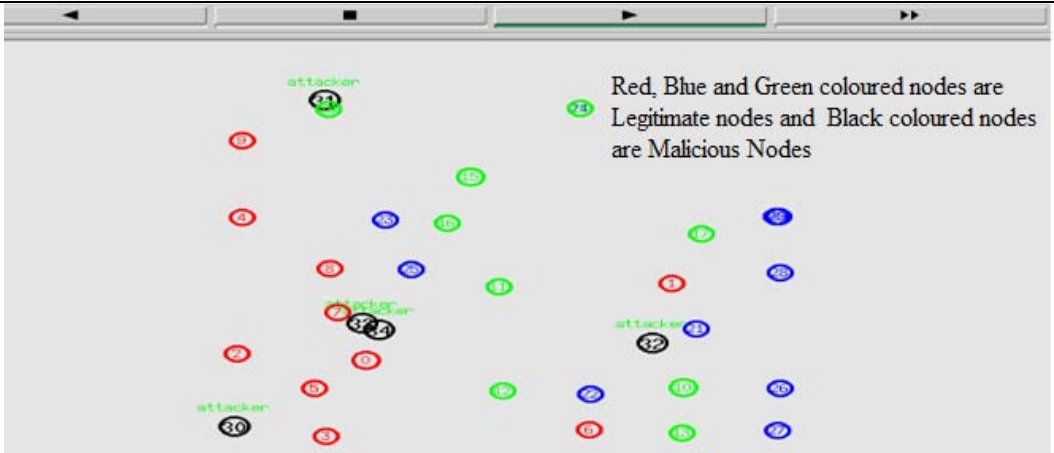

Fig. 3. Simulation Model with 35 nodes

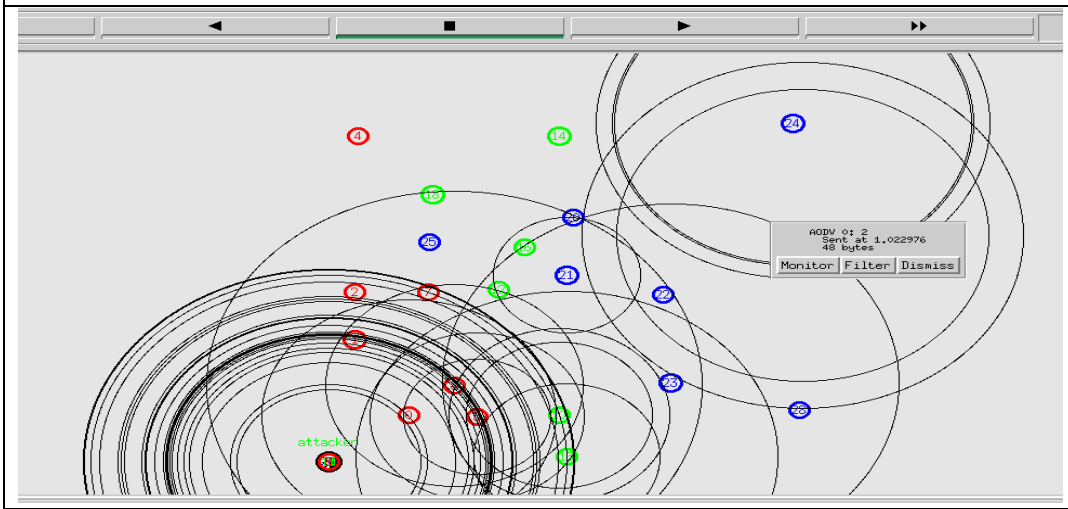

Fig. 4. AODV Routing Protocol

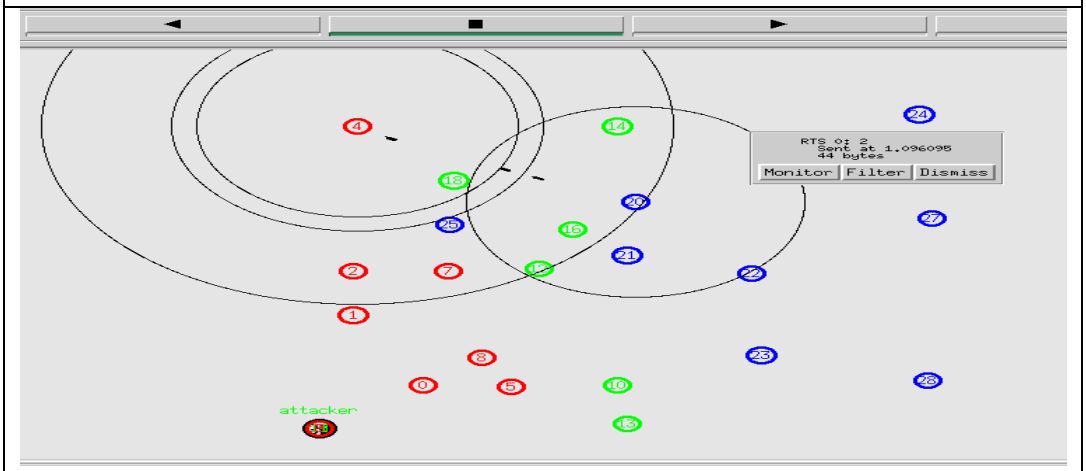

Fig. 5. Request to Send control signal

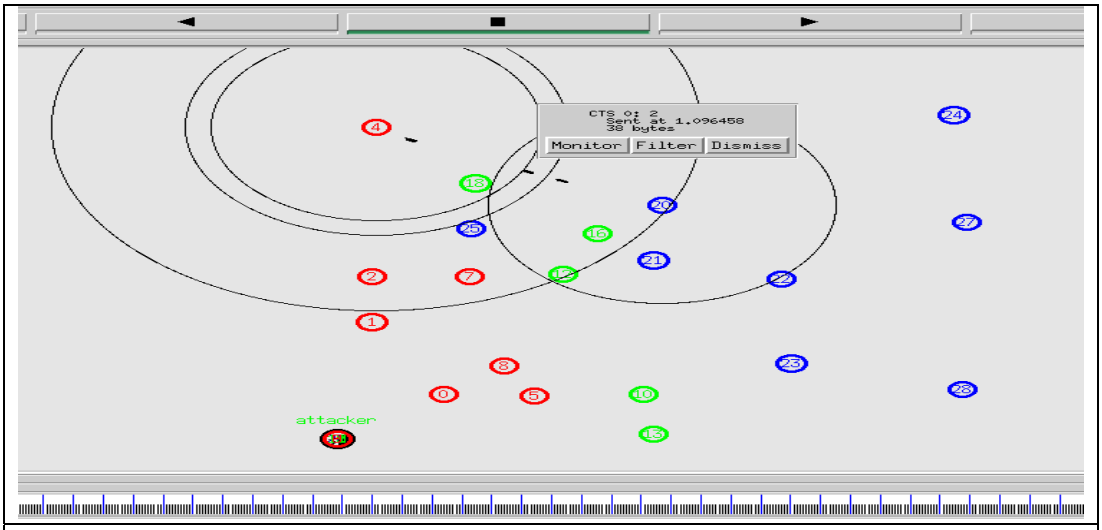

Fig. 6. Clear to Send signal

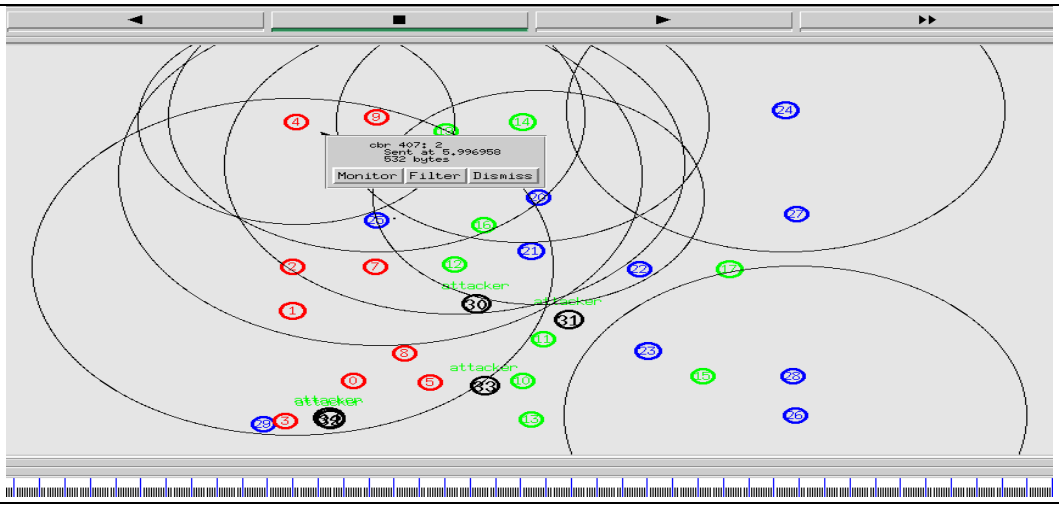

Fig. 7. Constant Bit Rate Data Packets

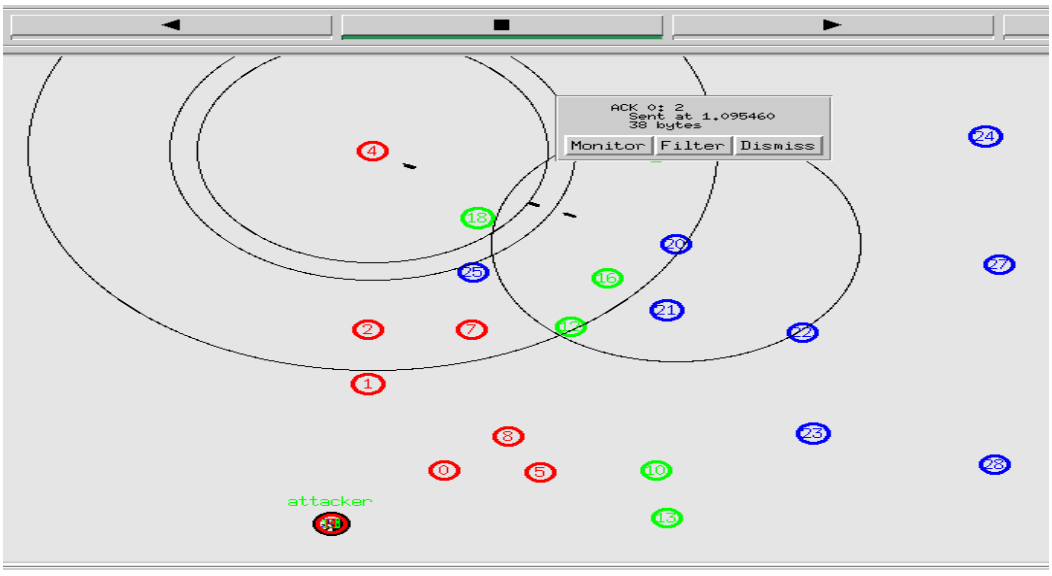

Fig. 8. Acknowledgement Signal

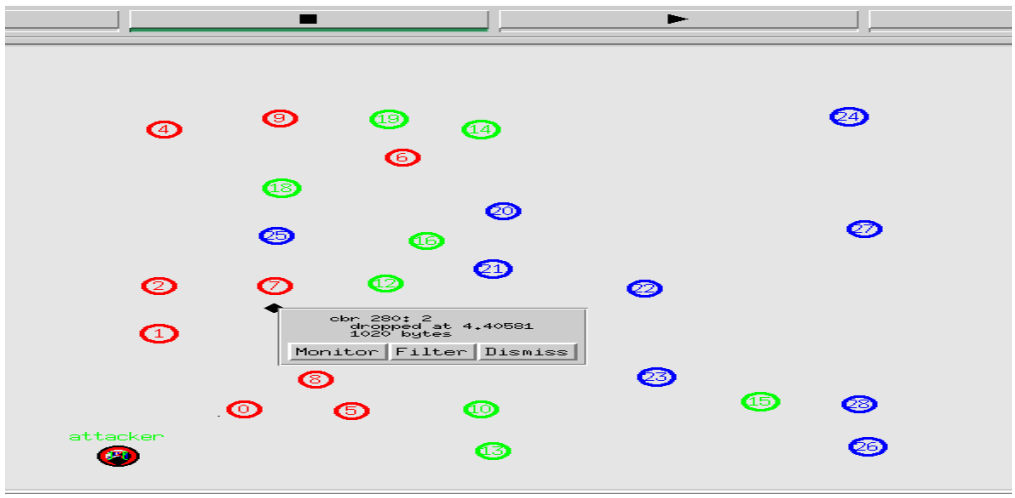

Fig. 9. Packet dropped at node

4. Results

Simulation is done using 35 nodes and the results are tabulated in the Table 2. The simulation results of various network parameters like throughput, packet loss and delay are calculated. The parameters show better performance for the Opinion Trust Algorithm when compared with the existing Compound MAC.

Delay (Sec)			Throughput(bps)			Packet Loss		
	Opinion Trust	Compound MAC		Opinion Trust	Compound MAC		Opinion Trust	Compound MAC
Time (Sec)	Delay32.tr	Delay02.tr	Time (Sec)	Out32.tr	Out 02.tr	Time (Sec)	Lost32.tr	Lost02.tr
0	0	0	0	0.0	0.0	0	0.0	0
3.5	0.12	0	3.5	244800.0	0	3.5	226.0	0
5	0.06	0	5	89760.0	0	5	0.0	0
6.5	0.08	0	6.5	89760.0	0	6.5	176.0	0
10	0.07	0.02	10	89760.0	170240.0	10	0.0	0
15	0.06	2.19	15	179520.0	8512.0	15	0.0	56
20	0.05	0.05	20	163200.0	72352.0	20	0.0	42
25	0.06	0.09	25	155040.0	38304.0	25	0.0	0
30	0.06	0.26	30	171360.0	29792.0	30	0.0	0
35	0.06	0.14	35	146880.0	34048.0	35	0.0	0
40	0.06	0	40	171360.0	0.0	40	0.0	0
45	0.06	0.04	45	73440.0	106400.0	45	0.0	0
50	0.06	0.04	50	171360.0	89376.0	50	0.0	0
55	0.06	0.05	55	155040.0	80864.0	55	0.0	0
59.5	0.06	0	59.5	0.0	0.0	59.5	0.0	0

Table 2. Delay, Throughput and Packet loss of Opinion Trust Algorithm and Compound MAC

The delay as shown in Fig. 10.is observed to be reduced and almost constant when compared to the existing method. As increase in delay between transmission and reception indicates insecure transmission here a reduction in delay indicates secure transmission. Throughput is the number of data packets received over a period and the throughput varies depending upon the protocol maximum the throughput indicates better network performance. As shown in Fig. 11.the throughput is improved when compared with the existing methods. The number of packets dropped is given by packet loss which is also an indicator for eavesdropping. As shown in Fig. 12.the packet loss is reduced by this Opinion Trust Algorithm.

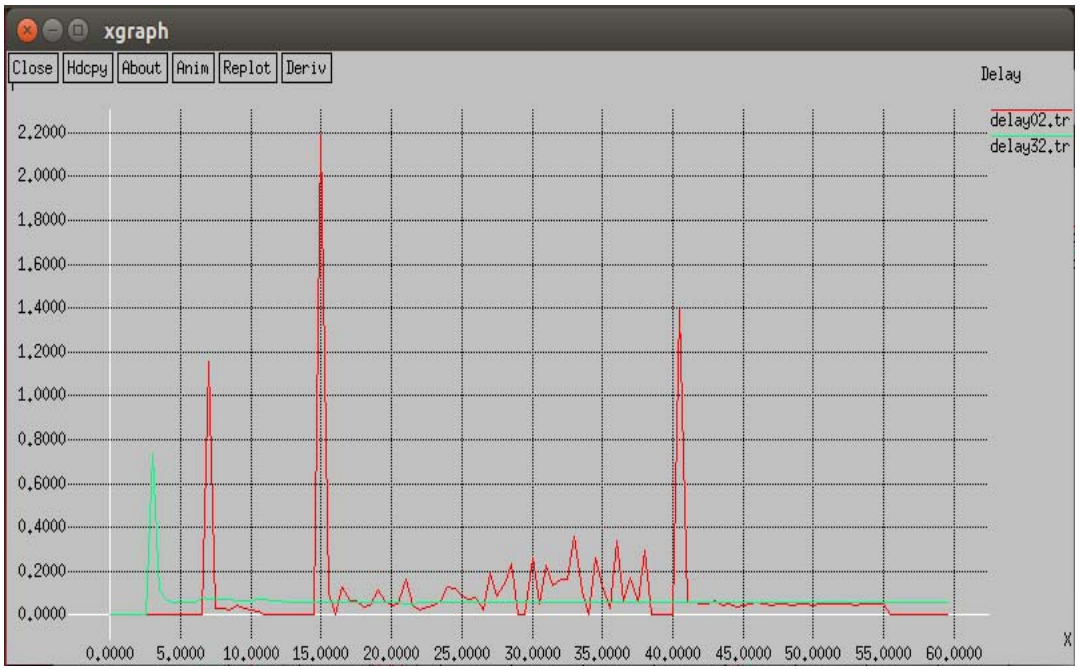

Fig. 10. Delay Comparison graph

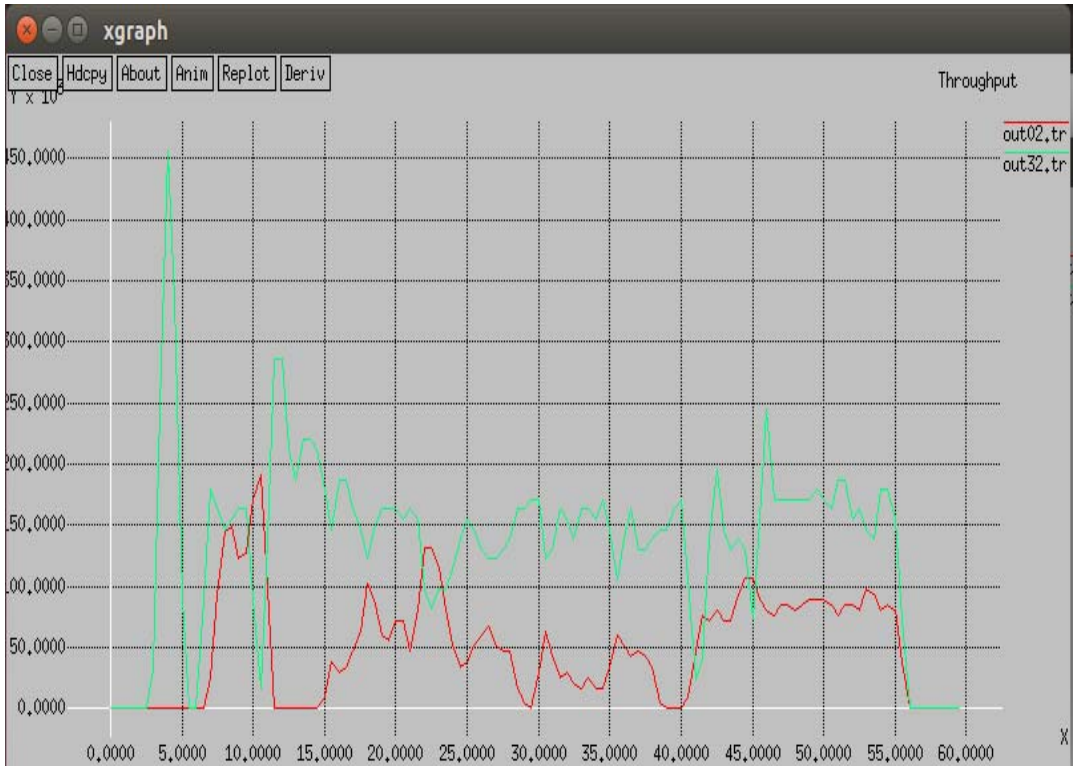

Fig. 11. Throughput Comparison Graph

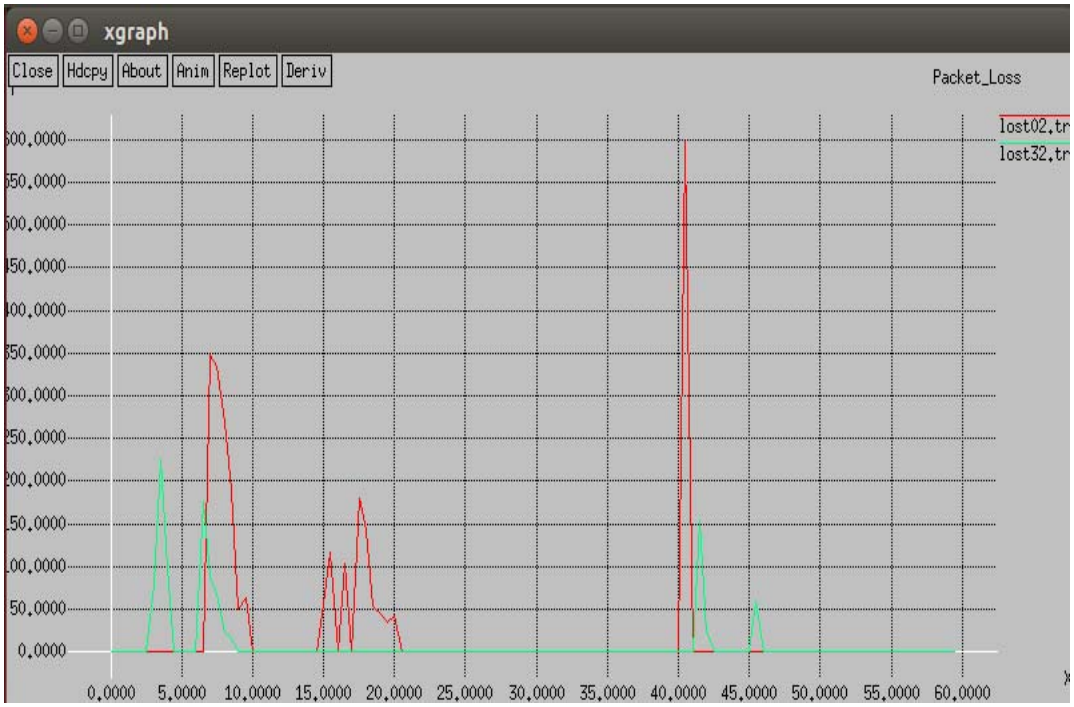

Fig. 12. Packet Loss Comparison Graph

5. Conclusion

An efficient physical layer security algorithm against eavesdropping was proposed in this paper. Performance parameters are evaluated through the simulations and proved that through Opinion Trust Algorithm the performance of the parameters improved drastically. Various studies indicate that there will be no algorithm that better represent all aspects of the result. Hence Opinion Trust Algorithm improves the performance in terms of packet loss and average delay effectively.

References

[1] A. Yener and S. Ulukus, "Wireless Physical-Layer Security:Lessons Learned from information Theory," Proc. IEEE, vol.103, no. 10, Oct. 2015, pp. 1814–25.
[2] H. Endo et al., "Free-space optical channel estimation for physical layer security," vol. 24, no. 8, pp. 46–51, 2016.
[3] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference- alignment-based wireless networks," IEEE Commun. Mag., vol. 54, no. 8, pp. 162–168, 2016.
[4] C. Sahin, B. Katz, and K. R. Dandekar, "Secure and robust symmetric key generation using physical layer techniques under various wireless environments," IEEE Radio Wirel. Symp. RWS, vol. 2016-March, pp. 211–214, 2016.
[5] J. Liu, Z. Liu, Y. Zeng, and J. Ma, "Cooperative jammer placement for physical layer security enhancement," IEEE Netw., vol. 30, no. 6, pp. 56–61, 2016.
[6] X. Lu, R. C. de Lamare, and K. Zu, "Successive optimization Tomlinson-Harashima precoding strategies for physical-layer security in wireless networks," Eurasip J. Wirel. Commun. Netw., vol. 2016, no. 1, 2016.
[7] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure Green Communication via Untrusted Two-Way Relaying: A Physical Layer Approach," IEEE Trans. Commun., vol. 64, no. 5, pp. 1861–1874, 2016.
[8] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving Physical Layer Security Using UAV-Enabled Mobile Relaying," IEEE Wirel. Commun. Lett., vol. 6, no. 3, pp. 310–313, 2017.
[9] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM Physical Layer Encryption Scheme," IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2114–2127, 2017.
[10] T. Yang, R. Zhang, X. Cheng, and L. Yang, "Graph based resource allocation for physical layer security in full-duplex cellular networks," IEEE Int. Conf. Commun., 2017.
[11] J. Ji, G. Zhang, W. Li, L. Sun, K. Wang, and M. Xu, "Performance analysis of physical-layer security in an OCDMA-based wiretap channel," J. Opt. Commun. Netw., vol. 9, no. 10, pp. 813–818, 2017.
[12] W. Lu, Y. Jiang, C. Yin, X. Tao, and P. Lai, "Security Beamforming Algorithms in Multibeam Satellite Systems," pp. 1272–1277, 2017.
[13] D. Tubail, M. El-Absi, S. S. Ikki, W. Mesbah, and T. Kaiser, "Artificial Noise-Based Physical-Layer Security in Interference Alignment Multipair Two-Way Relaying Networks," IEEE Access, vol. 6, pp. 19073–19085, 2018.
[14] J. Hua, S. Jiang, W. Lu, Z. Xu, and F. Li, "A Novel Physical Layer Encryption Algorithm Based on Statistical Characteristics of Time-Selective Channels," IEEE Access, vol. 6, pp. 38225–38233, 2018.
[15] H. A. Shah and I. Koo, "A Novel Physical Layer Security Scheme in OFDM-Based Cognitive Radio Networks," IEEE Access, vol. 6, pp. 29486–29498, 2018.
[16] M. Li, G. Zhang, G. Li, H. Li, and X. Zhang, "Secure Transmission Algorithm Based on Subcarrier Sorting and XOR Operation in OFDM Systems," 2018 IEEE Int. Conf. Commun. Syst. ICCS 2018, pp. 147–151, 2018.

[17] S. Li et al., "Secure Strategy for OFDM-PON Using Digital Chaos Algorithm with Fixed-Point Implementation," J. Light. Technol., vol. 36, no. 20, pp. 4826–4833, 2018.
[18] H. S. Gill, S. S. Gill, and K. S. Bhatia, "A novel approach for physical layer security in future-generation passive optical networks," Photonic Netw. Commun., vol. 35, no. 2, pp. 141–150, 2018.
[19] C. Ouyang, Z. Ou, L. Zhang, and H. Yang, "Optimal Transmit Antenna Selection Algorithm in Massive MIMOME Channels," IEEE Wirel. Commun. Netw. Conf. WCNC, vol. 2019-April, pp. 1–6, 2019.
[20] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV Communications via Joint Trajectory and Power Control," IEEE Trans. Wirel. Commun., vol. PP, no. c, p. 1, 2019.
[21] S. Wang, X. Xu, K. Huang, X. Ji, Y. Chen, and L. Jin, "Artificial noise aided hybrid analog-digital beamforming for secure transmission in MIMO millimeter wave relay systems," IEEE Access, vol. 7, pp. 28597–28606, 2019.

Authors 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 12 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 22 years of teaching experience and presently working as an Head of Department in Electrical, Electronics and Communication Engineering Department in GITAM School of Technology ,Hyderabad.. Her areas of research include Wireless Networks, Wireless Sensor Networks and Wireless Communications. She had publications in various national and International Journals. She was a Board member for various reputed journals**.**