ISSN No.: 2454- 2024 (online)

International Journal of Technical Research & Science

DETECTION AND ISOLATION MECHANISM OF JAMMING ATTACK FOR AODV IN MANET

Aditi[*] and Joy Karan Singh[**]

sweetgagan608@gmail.com[*], joysachar@gmail.com[**]

Department of CSE CT Institute of Technology and Research Maqsudan, Jalandhar (Punjab), India

Abstract- The mobile ad-hoc network is the self configuring type of network in which mobile nodes can change its location any time. Due to its decentralized nature, much type of active and passive attacks is possible in the network. Jamming is the active type of attack which degrades network performance in terms of throughput, Packetloss, Retransmission attempts, Delay and PDR. In this work, novel technique is been proposed which will detect and isolate malicious nodes from the network. The proposed technique will be based on monitor mode and threshold. The simulation is been performed in NS2 and it is been analyzed that proposed technique performs well in terms of throughput, Packetloss, Retransmission attempts, Delay and PDR.

Keywords- AODV, Attacks, Jamming, MANET, QoS parameters.

1. INTRODUCTION

The communication between computers with the help of standard network protocols is known as wireless networking technology. The communication is done without using any external cables in the network and the transmission is done through radio waves at the physical level. This network is also known as Wi-Fi or WLAN. The communication between two devices in this network can be done through radio frequency. The IEEE standard for wireless network is 802.11. There are two types of Wireless Operating modes:

- Infrastructure Mode
- Ad-hoc Mode or Infrastructure less Mode

Here, the communication in the infrastructure based network takes place between the wireless nodes and the access points and no direct communication is done between the wireless nodes. The medium access is handled by the access point and this access point acts as a bridge in between the wireless and wired networks. Fixed numbers of base stations are used in this network and if any node goes out of range of a particular base station, another base station comes in the range. Cellular networks are an example of the infrastructure based networks. In this network the infrastructure is centralized based and the controlling activity is done by the controller such as a router. On the contrary, the infrastructure less network does not require ant parameters for design and working. The communication with other nodes in this network can be done directly and there is no access point needed for controlling the medium access. All the nodes available in this network act as routers and are capable of moving. These nodes can also be connected dynamically in an arbitrary manner [6].

MANET (mobile ad hoc network) is a robust infrastructure less wireless network which is formed either by all mobile nodes or by both fixed as well as mobile nodes. Arbitrary topology is formed by connecting nodes randomly amongst each other. The nodes can act either as routers or as hosts. The nodes have the property of self-configuration which can be helpful in providing communication in areas where it is difficult to communicate. There is need of both static as well as dynamic routing protocols in MANET. In an ad hoc network there is no centralized infrastructure available which results in imposing great challenge to the functionality of the network. To avoid this, MANETs are proposed which have the property of accepting and routing traffic from the intermediate nodes towards the destination. The nodes cannot act both as the routers as well as hosts. Energy constraint occurs in the network if there is frequent breakage of connection and re-connecting found in the network. The routing protocols that are used for communication play a very important role in this network. This is due to the fact that there is a huge impact on the complete network due to these routing protocols.

In this paper, we esteem a particular category of DoS attacks called Jamming. In actual fact, the mobile host in mobile ad hoc networks is a part of wireless medium. Thus, the radio signals can be jammed or interfered, which make the message to be amoral or missed. If the attacker has a strong transmitter, a signal can be launched that will be strong enough to conquer the directed signals and distort communications. There are several attack schemes that a jammer can do in order to interfere with other wireless communications. In proposed work we implemented ad-hoc on demand distance vector routing protocol on wireless sensor network because it select the shortest path for transferring data source to destination. But it cannot isolates jamming effectively. To increase the performance of the network and enhance the performance of AODV Watch dog technique is used. Watchdog is a monitoring technique [3] which detects the misbehaving nodes in the network. . In this work Watchdog algorithm is implemented on AODV to detect the selfish node form the network. So, we implemented, analysis and compare the result of Watchdog technique with Adhoc- On Demand Distance Vector Routing Protocol. Watchdog algorithm in previous work implemented on mobile Adhoc network for avoiding jamming. We implemented Watchdog algorithm on AODV then analyze and compare the results with AODV jamming. Enhanced Watchdog technique is my proposed work which having increase the performance of network and AODV as well as decrease the chances of jamming. Lastly, we would like to analyze and compare the results of proposed technique Enhanced Watchdog technique with exiting Watchdog technique and AODV. By proposed Watchdog technique with other two I want to observe the difference between the performances of enhanced Watchdog technique, exiting Watchdog technique and AODV.

2. REVIEW OF LITERATURE

In paper [1] Caimu Tang et.al proposed efficient authentication mechanisms for low-power devices. In the proposed scheme the mobile station only need to pass one packet for mutual authentication. They used the elliptic-curve-crypto system based trust delegation Mechanism to generated group pass code for mobile station authentication. The authentication mechanism is helpful in preventing networks from various active and passive attacks. The authentication of devices is done through the exchange of one packet while visiting the base station. When compared to the other authentication methods proposed, this method involves less computations and message exchange.

In paper [2] Jacek Cicho et.al discussed the problem of efficient alarm protocol for ad-hoc radio networks. These networks consist of devices that try to gain access through a shared radio communication channel which is used for transmission purpose. At any instance, there might be a sudden requirement of alerting the target user regarding any dangerous radiations of any type. For this purpose, a protocol which uses O (log n) time slots is used. This protocols shows that (log n= log n) is a lower limit for the time slots involved.

In paper [3] Priyanka Goyal et.al discussed about the Mobile ad-hoc networks which are now used in various fields for evolving the research and development of wireless networks. There are various challenges faced by MANET which are to be resolved by enhancing the special properties of MANET. In this paper, the features, categories as well as vulnerabilities of MANET are mentioned for getting detailed view about these networks. Towards the end, the emerging applications as well as the future enhancements to be proposed in MANET are also mentioned.

In paper [4] Liu et al. proposed a novel two-phase jamming detection method for sensor networks. In first phase, some signs of jamming are identified speedily. When signs are found then second phase of detection is applied. In this technique we don't requires any extra communication or hardware.

In paper [12] Babar et al. represented the game theoretic model of the jamming attack. This paper suggested a game theory based detection technique which is utilized to detect all kinds of jamming attack. This method provides better performance in words of delay, energy and throughput also.

In paper [13] S. T. et al. represented a profile based technique which is utilized to detect and suspend the flooding attack on MANET with the help Adhoc on Demand Distance Vector (AODV) routing protocol. In this technique every single node has a profile value. These profile values are put on the base of behavior of MANET. Whenever the node attempts to overreach the fixed threshold value, the attack will be identified and isolated. The key benefit of this technique is that threshold value is not defined; it is based on the average request permitted in the network which changed with the number of request in the network .

3. ATTACKS IN MANET

Providing better security solutions to the wireless ad-hoc network is a major challenge in MANETs. For this purpose, it is important to study all the attacks that are possible to occur while there is data transmission occurring in the network. Numerous types of attacks are found in MANET. Basically the classification of attacks is done in two parts:

3.1 Active Attack

Active attacks are of two types, internal attacks and external attacks. These types of attacks affect the performance of the network. The tasks performed are also affected as the modified data could also be sent which might be a false message.

- **Internal attacks:** These types of attacks are found within the network. The attacker nodes are found within the network and these nodes take unauthorized access. They behave as normal nodes and thus disrupt the network on authentication base. The traffic in between the other nodes is also analyzed by these nodes and they begin to involve in various other activities of the network.
- **External attacks:** These types of attacks are made by the attacker nodes found outside the network. These nodes are not present within the network and create authentication issues from the outside. The examples of these types of attacks are: jamming, modification and message reply.

3.2 Passive Attacks

Passive attacks are attacks that are difficult to find on the network and does not disturb the network task, performance and actions. The most common example of passive attacks is traffic analysis and traffic monitoring.

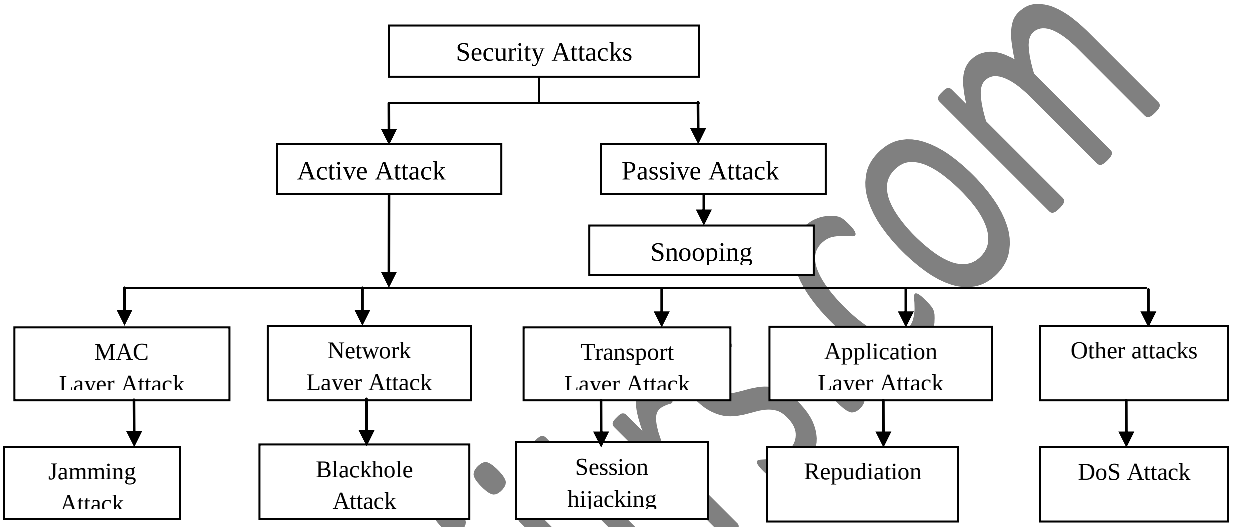

Fig. 3.1 Security Attacks for Different Layers

Fig 3.1 describes the security attacks, there are two types of security attacks one is active attack and other is the passive attack. The common passive attack is the snooping. Active- attacks are five types such as attack on MAC layer, network layer, transport layer, application layer and other attacks. The attack on MAC layer is Jamming attack. The attacks on network layer are black-hole, wormhole and Gray-hole attack. The attack on Transport layer is Session hijacking. The attack on Application layer is Repudiation. The other attacks are DoS attack and Device tempering.

3.3 Jamming Attack

The jammer is an entity with the aim of attempting to involve in the sending and receiving of data within the wireless communications of network. For blocking the legal traffic of the wireless channel, the jammer continuously emits RF signals [2]. A ratio of the number of packets sent out by any justifiable traffic source to the number of packets to be sent by the MAC layer is taken. This attack has a number of sources instead of just one source. These sources send the rough packets to the transmission channels and to the jammed channels as well. This results in packet loss which further decreases the efficiency and reliability of the system. The problems such as the unavailability of free channel, delay in transmission and new packet drops due to the absence of buffer space are seen.

Physical Jamming (Physical Layer): Another simple however, disruptive form of DoS attack is the Physical or Radio jamming found in the wireless networks. The reasons behind such attacks are the continuous emission of radio signals or the sending of random bits to other channels. The monopolizing of the wireless medium can be done for causing such attacks by the jammers which can result in denying a complete access to the channel. The channel is to be made idle and the carrier sensing time required is usually large. The nodes enter into a large exponential back-off period, so this results in affecting the adverse propagating affect.

Virtual Jamming (MAC Layer): The virtual carrier sensing is utilized in IEEE 802.11 for checking the availability of the wireless medium. The attacks on RTS/CTS frames or the DATA frames can be used for introducing jamming at the MAC layer. The MAC layer provides a benefit of providing the adversary node to consume less power while it targets these attacks. The consumed power is less as compared to the physical radio jamming. In this paper, the

DoS attacks made at the MAC layer are discussed. These attacks result in collision of RTS/CTS control frames or DATA frames.

4. PROPOSED METHODOLOGY

A partial DoS attack which is triggered by the malicious nodes in the network is known as jamming packet. The affects of jamming attack are that the throughput of the network gets reduced as well as the delay is increased at a steady rate. In this work, the jamming attack of AODV protocol is detected and isolated. The route is established between source and destination on the basis of hop counts and sequence numbers. The malicious node exists in the route which is act as source or multiple sources. The malicious node will be responsible for triggering the jamming attack. The proposed methodology will detect the malicious node and isolate, it from the network. The throughput of the network is of great concern in this methodology. The nodes go to the monitor mode once the threshold of the network degrades to certain threshold value. This helps in detection of the malicious node. From the source side, the ICMP packets that are generated flood in the network. These packets further act as the monitor nodes. The monitoring nodes detect the malicious node which is not further sent to the destination. When the malicious node is detected by the nodes, the reply is sent to the source node. The path is isolated to the source which stops forwarding more packets further.

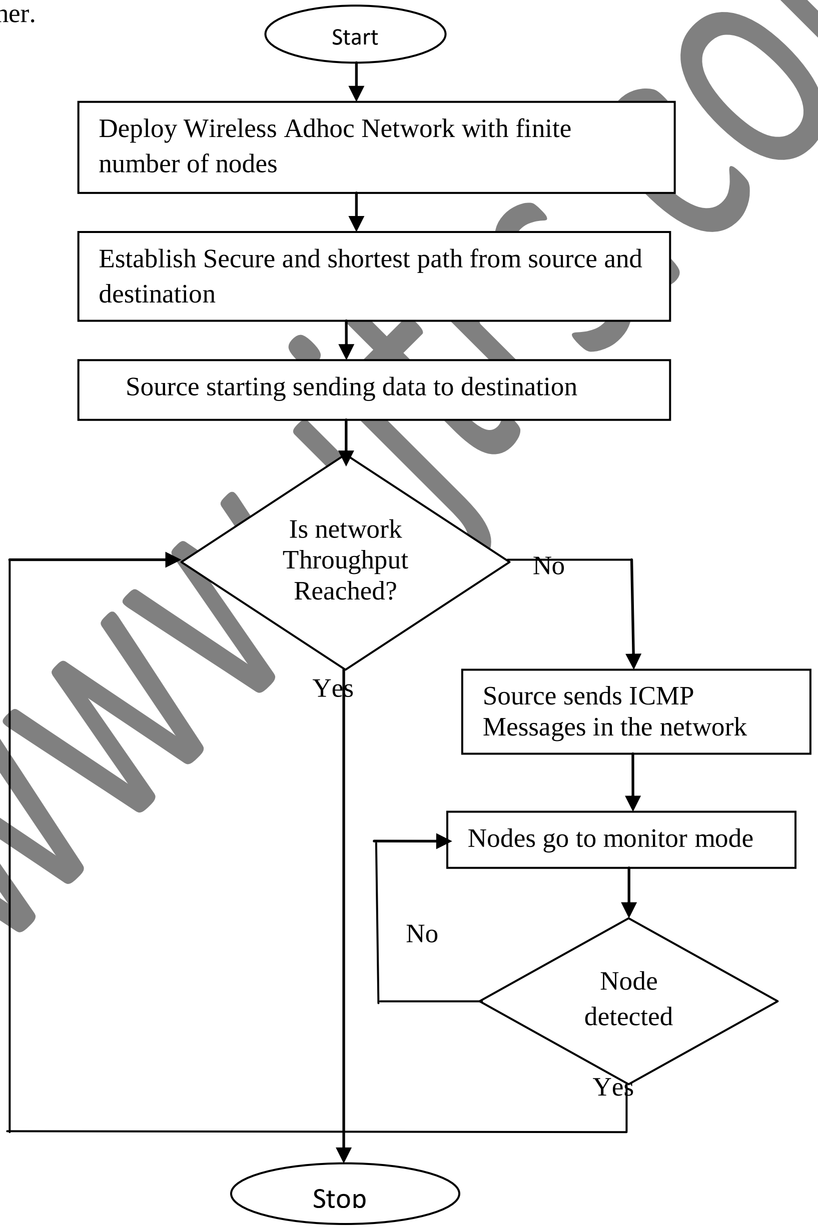
Start
Deploy Wireless Adhoc Network with finite number of nodes
Establish Secure and shortest path from source and destination
Source starting sending data to destination
Is network Throughput Reached?
No
Yes
Source sends ICMP Messages in the network
Nodes go to monitor mode
No
Node detected
Yes
Stop

Fig. 4.1 Flowchart of Proposed Technique

5. EXPERIMENTAL RESULTS

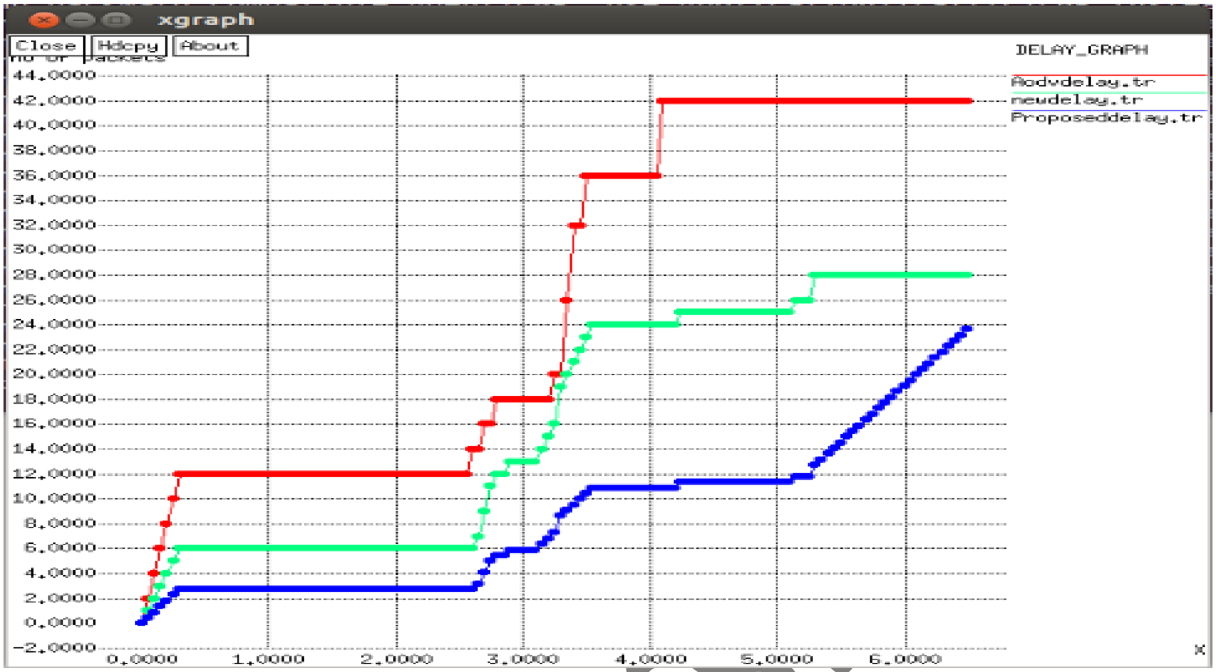

Fig. 5.1 Delay Graph

As shown in fig. 5.1, Delay graph is represented. Red line shows AODV delay, green lines shows previous delay and blue lines shows proposed energy. In proposed system delay is less as compared to the existing system. So the new technique is more efficient.

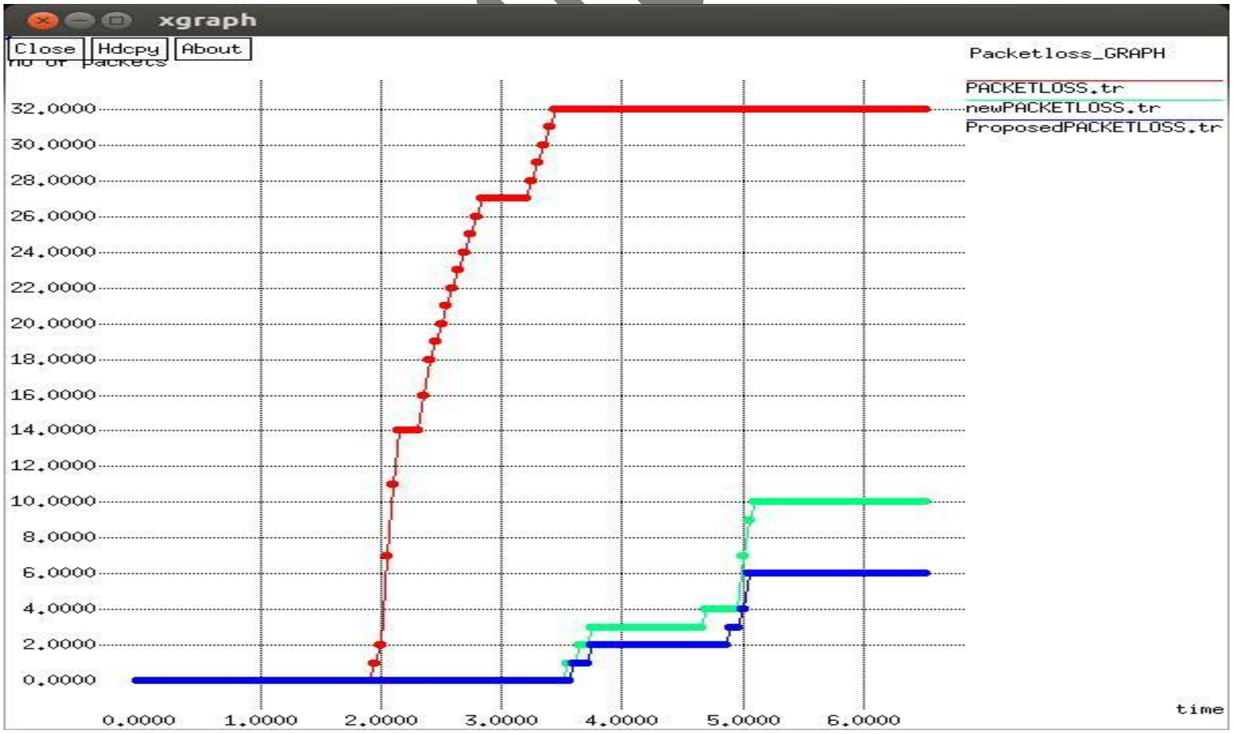

Fig. 5.2 Packet Losses Graph

As shown in fig. 5.2, packet loss is less in new proposed than the existing system. Blue lines shows less packet loss of new system and Green lines shows more packet loss in existing system.

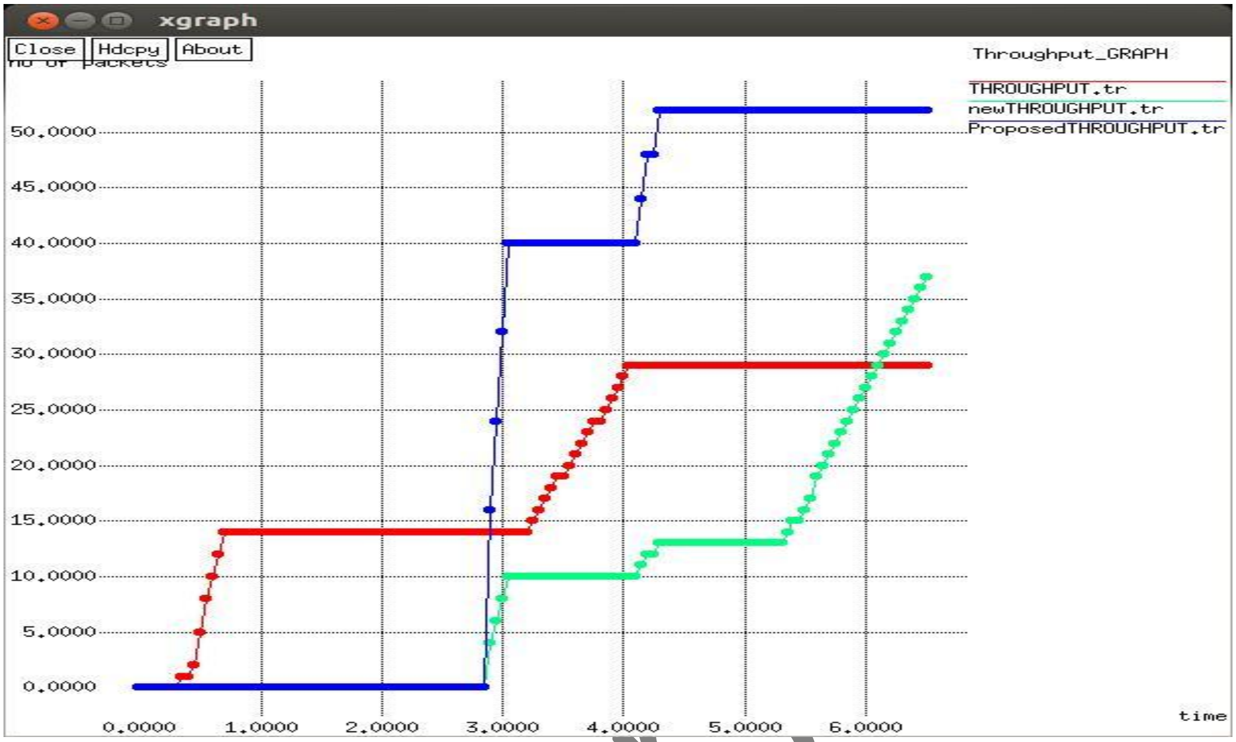

Fig. 5.3 Throughput Graph

As illustrated in fig. 5.3, the throughput of the AODV, proposed and existing algorithms is compared. It is been analyzed that network throughput is high when the attack is isolated from the network.

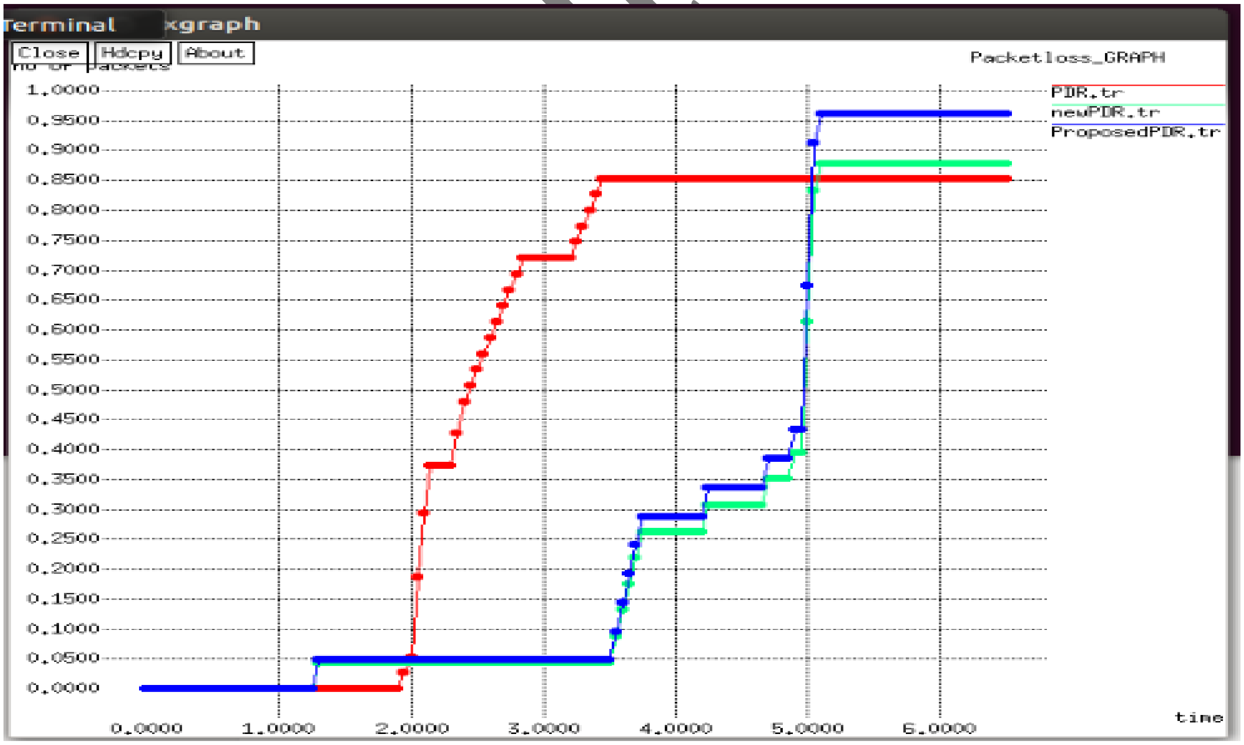

Fig. 5.4 PDR Graph

As shown in fig. 5.4, the PDR of the proposed and existing algorithms are compared to analyze network performance. It is been analyzed that PDR of the proposed algorithm is increased at steady rate after attack isolation in the network.

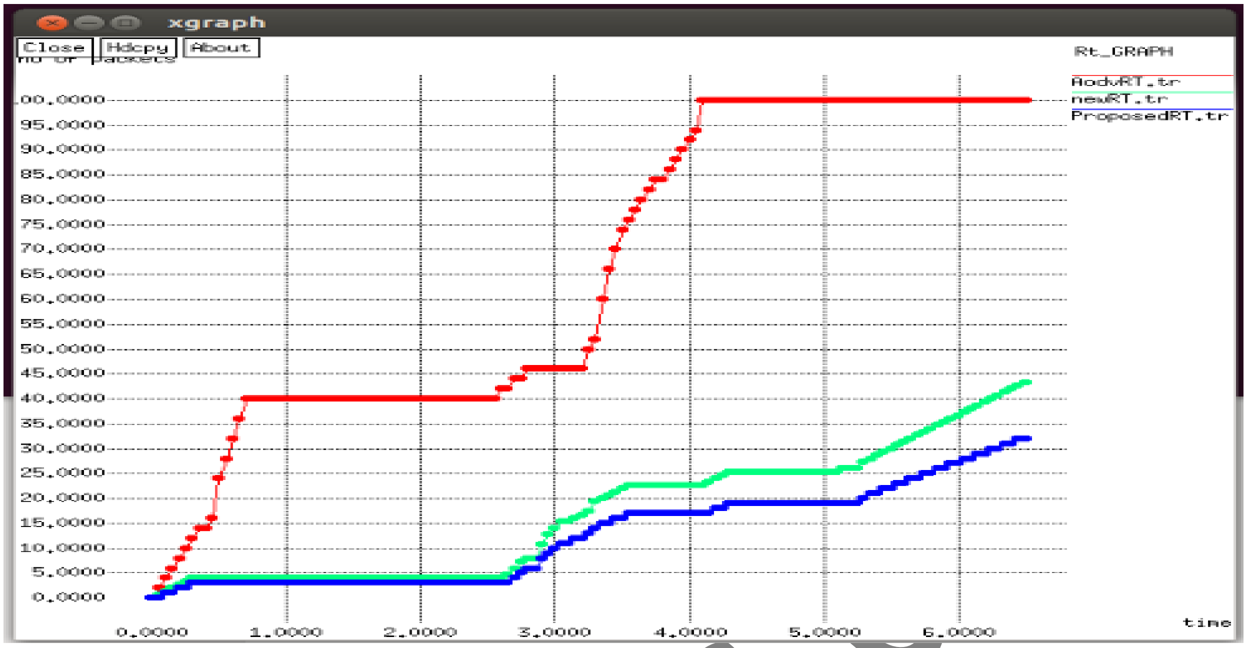

Fig. 5.5 Retransmission Attempts Graph

As shown in fig. 5.5, the retransmission attempts of the AODV, proposed and existing algorithms are compared to analyze network performance. It is been analyzed that retransmission attempts of the proposed algorithm is decreased at steady rate after attack isolation in the network.

Table 4.1 Comparison of Technique

Parameter	AODV Jamming (packet/sec)	Old algorithm (packet/sec)	New Algorithm (packet/sec)
Delay	42	28	24
Packetloss	25	9	6
Throughput	29	37	53
PDR	0.85	0.88	0.96
Retransmission attempts	100	44	33

From the Table 4.1, it is represented that the performance computed in the case of the purposed algorithm is better as compared to old algorithm. While using the same parameters, the throughput in proposed approach is better than the existing approach.

CONCLUSION

In this paper, it is concluded that the demand of monitoring nodes prevent the various inside and outside attacks. We evaluate the ICMP protocol for authentication. In our work, we propose a new technique to isolate attack between the mobile nodes. We implement new proposed technique and compare the results with the previous techniques. Experimental Result shows that proposed technique is better than existing technique.

REFERENCES

[1] Caimu Tang ,Dapeng Oilver,“ An Efficient Mobile Authentication Scheme for Wireless Networks”, IEEE, vol 7, issue 4, **(2010),** pp. 1408 - 1416.

[2] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada “On Alarm Protocol in Wireless Sensor Networks”, 9th International Conference, volume 6288, ISSN: 0302-9743, **(2010)**, pp 43-52.

[3] Priyanka Goyal, Vintra Parmar and Rahul Rishi ,“ MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, ISSN (Online): 2230-7893 **(2011),** pp. 345-358.

[4] D. Liu, J. Raymer, A. Fox “Efficient and Timely Jamming Detection in Wireless Sensor Networks” in 9th International Conference on Mobile Adhoc and Sensor Systems MASS, page 335-343. IEEE Computer Society, December 2012.

[5] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Applications and Challenges”, IJSER, volume 3, issue 3, **(2005),** pp. 60-66.

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, Springer, **(2006)**, pp 103-135.

[7] Sevil Şen, John A. Clark, Juan E. Tapiador, “Security Threats in Mobile Ad Hoc Networks”, IEEE, **(2010).**

[8] Rusha Nandy, “Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme” Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, **(2011),** Pages: 1035-1043.

[9] Wenjia Li and Anupam Joshi , “Security Issues in Mobile Ad Hoc Networks- A Survey”, **(2005)**.

[10] Vinit Garg, Manoj Kr.Shukla, Tanupriya Choudhury, Charu Gupta, “Advance Survey of Mobile Ad-Hoc Network,” IJCST Vol. 2, Issue 4, **(2011),** ISSN: 2229-4333.

[11] Humayun Bakht,“ Survey of Routing Protocols for Mobile Ad-hoc Network” , International Journal of Information and Communication Technology Research, Volume 1 No. 6, **(2011),** ISSN-2223-4985.

[12] S. D. Babar, N. R. Prasad, R. Prasad “Game Theoretic Modelling of WSN Jamming Attack and Detection Mechanism” Published in Wireless Personal Multimedia Communications (WPMC), 2013.

[13] Rajakumar P., Prasanna T., and Pitchaikkannu A. "Security attacks and detection schemes in MANET," Electronics and Communication Systems (ICECS), 2014 International Conference on IEEE, 2014.