Trust Based Mechanism for Isolation of Jelly Fish Attack in MANETs

[1]Gurinder Kaur, [2]Jasvir Singh
[12]*Department of Computer Engineering, Punjabi University, Patiala*

***Abstract*—**The mobile adhoc is the decentralized type of network in which no central controller is present. The routing, security and quality of services are the three issues of MANETs. The routing protocols are broadly classified into reactive, proactive and hybrid. In this paper, the AODV, DSR and DSDV routing protocols are compared and it has been analyzed that AODV is the best performing protocol. The security attacks are classified into active and passive which is triggered by the malicious node present in the network. The jelly fish attack is the active type of attack which reduce network performance in terms of various parameters. The novel technique is proposed which is the trust based technique of the detection of malicious nodes in the network. The proposed technique is implemented in NS2 and performance is analyzed is analyzed in terms of various parameters

***Keywords*—**AODV, DSR, DSDV, Trust, Malicious node

I. INTRODUCTION

In day-to-day communication wireless networks plays a prominent role. There are many applications where it is widely used like military applications, industrial applications and in personal area networks. In coming generation, MANET will be widely used in various applications due to its independent nature. It can join and leave network any time. Topology of the network changes dynamically and covers wide geographically area of network for communication. Because of its decentralized nature its scalability is better than infrastructure network. In any crucial scenarios such as military conflicts, natural disasters etc, ad-hoc network provides better performance due to the minimum configuration and quick operations [1]. MANET is a self configuring network, in which topology is dynamic. These nodes are struggling to cope with the normal effect of radio communication channels, multi-user interference, multi-path fading etc. The design of an optimum routing protocol for MANET is highly difficult. To determine the connectivity of network organizations, there is a need of an efficient algorithm link scheduling, and routing in such dynamic scenarios, becomes very important. The efficiency of a routing algorithm depends on the proficient and winning route computation [2]. There are a variety of attacks possible in MANET. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols. A passive attack does not disrupt the normal operation of the network. The attacker only snoops the data exchanged in the network without altering it. It includes Eavesdropping, jamming and traffic analysis and monitoring. In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network. Active attacks can be internal or external [3]. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks .The ultimate goals of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, and availability to mobile users.

A. Black hole attack

According to this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. When the attacker receives a request for a route to the destination node, it creates a reply message which advertises itself as a valid path to destination [4]. The attacker consumes the intercepted packets without any forwarding.

B. Gray hole Attack

The gray hole attack is also termed as misbehaving attack. In this attack, the attacker selectively drops the packet with certain probability. Also, in this attack the intruder node behaves maliciously for the time it selectively drops the packets and then switches to its normal behaviour.

C. Wormhole attack

In this attack, an attacker records the packets at one location in the network and tunnels them to another location [5]. The routing can be disrupted when routing control messages are tunnelled. This tunnel between two colluding attackers is referred as a wormhole.

D. Byzantine attack

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services.

II. JELLY FISH ATTACK

Jelly Fish attack is concerned with transport layer of MANET stack. The JF attacker disrupts the TCP connection which is established for communication. Jelly Fish (JF) attacker wishes to intrude into forwarding group and then it delays data packets unnecessarily for some amount of time before forwarding them [6]. Due to JF attack, high end to end delay takes place in the network. So the performance of network (i.e. throughput etc) decreases substantially. Application i.e. file transfer requires reliable and congestion controlled delivery. It is provided by Transmission Control Protocol (TCP). JF attacker disrupts the whole functionality of TCP, so performance of real time applications become worse.

III. LITERATURE REVIEW

S.S Tyagi et al. [7] have provided the simulation based comparison and performance analysis on different parameters like PDF, Average end to end delay, Routing Overheads and Packet Loss. Analysis and investigations are conceded out on three prominent protocols, AODV, DSR and DSDV using ns2. DSDV is chosen as agent of proactive routing protocol while AODV and DSR are the agents of reactive routing protocols. As AODV protocol has thousand of nodes while DSR is designed up to two hundred nodes. In dense environment, AODV performed better except packet loss. DSR and AODV both performed well. AODV and DSR are proved to be better than DSDV.

Kavita Pandey et al. [8] have discussed that the performance of MANET routing protocols is examined with respect to following four performance metrics namely, throughput, average delay, number of packets dropped and routing overhead. DSDV is a proactive protocol, whereas, AODV and DSR falls under the category of reactive protocol and ZRP is a hybrid protocol. Experimental results show that there are some drawbacks of each protocol in different scenario. In terms of throughput, AODV performance is better than other protocols. It can also be concluded from the simulation results that the reliability of AODV and DSR protocols is better than other two protocols.

Vrutik shah, et.al (2014) proposed in this paper [9] that the recent advancement in the wireless technology and their wide-spread development have made remarkable enhancement in efficiency in the corporate and industrial and military sectors. The increasing popularity and usage of wireless technology is created a need for more secure wireless Ad hoc network. This paper aims and developed a new protocol that prevent wormhole attack as an Anti-worm protocol which is based on responsive parameters, that does not require as a significant amount of specialized equipment, trick clock synchronization, no GPS dependencies countermeasures.

A. Vani, et.al (2011) the infrastructure [10] of a mobile ad hoc network (MANET) has no router for routing, and all nodes must share the routing protocol to assist each when transmitting messages. This paper focuses on the wormhole attack poses the greatest threat and is very difficult to prevent; therefore this paper focuses on the wormhole attack, by combing three techniques. So the proposed scheme has three techniques based on hop count, decision anomaly, neighbour list count methods are combined to detect and isolate wormhole attacks in adhoc networks. That manages how the nodes are going to behave and which to route the packets in secured way.

Manjot Kaur, et.al (2014) explained [11] that Mobile Adhoc Networks have become a part and parcel of technology advancements due to its working as autonomous system. MANET networks are vulnerable to various types of attacks and threats due to its unique characteristics like dynamic topology, Shared physical medium, distributed operations and many more. There are many attacks which effect the functioning of MANETS' such as denial of service which is most commonly used to affect the network is one of the types of attacks in MANETS. Jellyfish attack has gained its name recently in attack scenario in Mobile Ad hoc networks. JellyFish Attack exploits the end to end congestion control mechanism of Transmission Control Protocol (TCP).

Mohammad Wazid et.al (2012) explained [12] that Jellyfish is a new denial of service attack. In JF delay variance attack, intruder node needs to intrude into forwarding group and then it delays data packets for some amount of time before forwarding. In this paper a comparative performance analysis of three reactive routing protocols i.e. AODV, DSR and TORA used in mobile ad hoc network is done under JF delay variance attack with increasing node density. If they have a mobile ad hoc network in which probability of occurrence of JF attack is high and also if it requires time efficient network service for information exchange with increasing number of nodes then they have to choose DSR protocol. If it requires high throughput and consistent service in the network with increasing node density then TORA protocol is recommended.

IV. RESEARCH METHODOLOGY

In this work, we are working on to check impact of jellyfish attack on various routing protocols like DSDV, AODV and DSR. It is been analyzed that AODV performance is high as compared to other routing protocols when jellyfish attack is triggered in the network. In this work, technique will be proposed which will detect and isolate from the network. The jelly fish attack will reduce the network performance and in technique will be proposed which is trust based technique for detection of malicious nodes from the network. In the proposed work, the trust of each node is calculated on the

basis of number of packets get forwarding in the network by node in the network. The node which forward maximum of packets has high trust as compared to the other node in the network. The node which has least trust is detected as the malicious node from the network.

$$T_A(B) = Q_A(B) + R(B) \quad (1)$$

Where TA(B) is trust computed by A about B, QA(B) represents the direct trust compute by about B, R(B) is the aggregated recommendations about node B by all its neighbors

V. PROPOSED ALGORITHM

Input : Network with Finite number of mobile nodes

Output : Detection of malicious node

1. Deploy wireless network with the finite number of nodes

2. Define source and destination node in the network

3. Establish path from source to destination using AODV protocol

4. Assign trust value of each node ()

Repeat for each node in the network

$$T_A(B) = Q_A(B) + R(B) \quad (1)$$

end

5. Repeat for all nodes in the network

Node with least trust is detected as malicious node

6. Apply Multipath routing for malicious node isolation

7. end

VI. RESULTS AND DISCUSSION

The proposed Algorithm is based on the detection of malicious nodes from the network. In this work, the network simulator version 2 used to implement proposed and existing scenarios. The simulation parameters are described in table 1

Parameter	Values
Antenna type	Omi-directional
Queue type	Priority queue
Number of nodes	24 nodes
Area	800*800 meters
Range	18 meter
Frequency	2.4 GHz

Table 1: Simulation Parameters

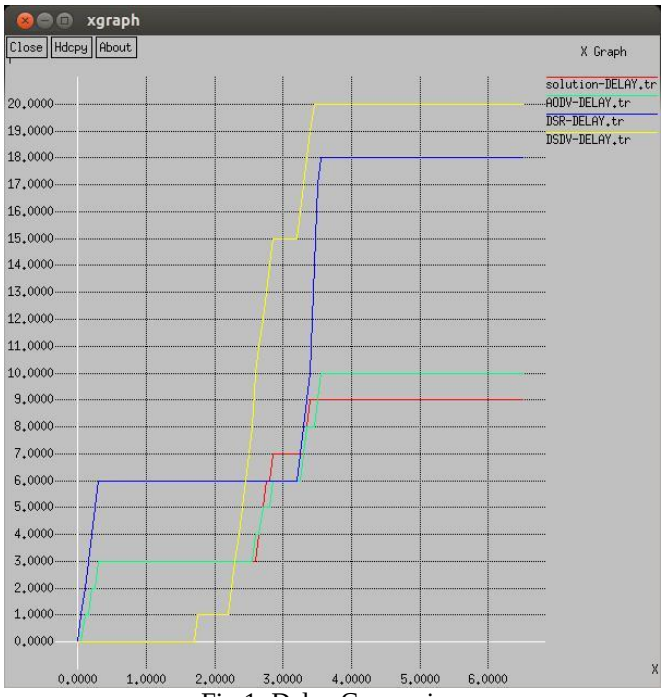

Fig 1: Delay Comparison

As shown in figure 1, Delay of the AODV, DSR , DSDV and Proposed technique is compared and it is been analyzed that due to isolation of jelly fish attack in the network delay of proposed technique is least as compared to other technique

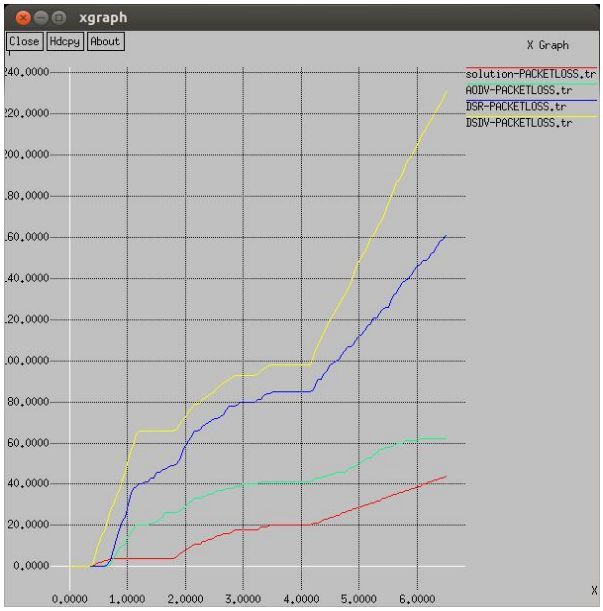

Fig 2: Packetloss Comparison

As shown in figure 2, the AODV, DSR , DSDV and proposed technique is compared in terms of packetloss. It has been

analyzed that network packetloss is reduced in the proposed technique as compared to other techniqes

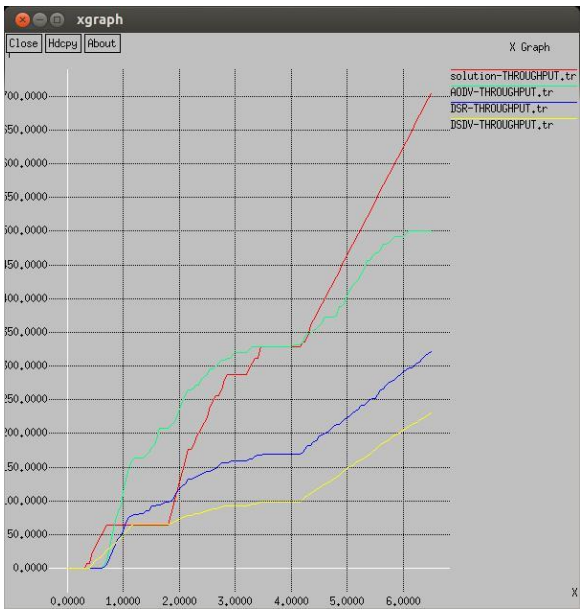

Fig 3: Throughput Comparison

As shown in figure 3, network throughput of AODV, DSR, DSDV and proposed technique is compared it is been analyzed that due to attack isolation network throughput is increased at steady rate.

VII. CONCLUSION

In this work, it has been concluded that AODV protocol is the best performing routing protocol among other routing protocols. The malicious nodes enter the network which triggers various types of active and passive attacks. In this paper, trust based technique is proposed which will detect and isolate malicious nodes from the network. The results are analyzed in terms of throughput, delay and packet loss which is improved in the proposed technique as compared to existing techniques.

VIII. REFERENCES

[1]. K. Majumder and S.K. Sarkar, "Performance analysis of AODV and DSR Routing Protocols in Hybrid Network Scenario", Proc. IEEE transactions on networking, Dec. 2009, pp. 1-4

[2]. S. Mohseni, R. Hassan, A. Patel, and R. Razali, "Comparative Review Study of Reactive and Proactive Routing Protocols in MANETs", 4th IEEE International Conference on Digital Ecosystems and Technologies 2010 IEEE, Apr. 2010, pp.- 304-309

[3]. S.S. Tyagi, R.K. Chauhan, "Performance analysis of ProActive and ReActive routing protocols for ad hoc networks", International journal of computer applications, Vol. 1, No.-14, 2010, pp. 27-30

[4]. T.P. Singh, Dr. R.K. Singh, J. Vats, "Effect of quality parameters on energy efficient Routing protocols in MANETs", Vol. 3 No-7, July 2011,pp. 2620-2626.

[5]. W. Kiess, M. Mauve, "A survey on real-world implementations of mobile ad-hoc networks", Vol. 5, Issue 3, Apr. 2007, pp 324-339

[6]. X. Hong, K. Xu, M. Gerla, " Scalable routing protocols for mobile ad hic networks", Network IEEE, Vol. 16, Issue 4, july 2002, pp. 11-21

[7]. S.S. Tyagi, R.K. Chauhan, "Performance analysis of ProActive and ReActive routing protocols for ad hoc networks", International journal of computer applications, Vol. 1, No.-14, 2010, pp. 27-30

[8]. K. Pandey, A. Swaroop, "A Comprehensive Performance Analysis Of Proactive, Reactive and Hybrid MANETs Routing Protocols", International Journal of computer Science Issues, Vol. 8, Issue 6, No 3, November 2011, pp. 432-441.

[9]. Internet Engineering Task Force, MANET working group charter.Available from: IETF MANET group Character Sector Jan. 2010

[10]. Mohammad Wazid, Vipin Kumar and RH Goudar, "Comparative Performance Analysis of Routing Protocols in Mobile Ad Hoc Networks under JellyFish Attack", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012

[11]. Manjot Kaur , Malti Rani, Anand Nayyar, "A Comprehensive Study of Jelly Fish Attack in Mobile Ad hoc Networks", , International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 199-203

[12]. S.A. Ade1& P.A. Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in MANET", International Journal of Information Technology and Knowledge Management, Vol. 2, No. 2, Dec. 2010, pp. 545-548