Secure Channel Establishment Algorithm for Isolation of Selective forwarding Attack in MANET

Hardeep Singh[1], Vinay Chopra[2]
[1]*Student*
[2]*Assistant Professor*
DAVIET

Abstract: The mobile ad-hoc network is the decentralized type of network in which mobile nodes join together and start communicating with each other. To establish path from source to destination various type of routing protocol are used which are broadly classified into reactive, proactive and hybrid type of routing protocols. The AODV is the best performing routing protocol in terms of routing overhead etc. Due to self configuring nature of network malicious nodes enter the network which are responsible to trigger active and passive attacks. The selective forwarding attack is the active type of attack in which malicious node is present in the path which drop some of the packets and some packets are forwarded to destination. In this paper, novel technique has been proposed which detect and isolate malicious nodes from the network. The simulation of proposed technique is done in NS2 and it performs well in terms of various parameters

Keywords: AODV, MANETs, Active, Passive, Selective forwarding attack

I. INTRODUCTION

Wireless communication is the level at which the transfer of user data over a distance without the use of "wired" or electrical conductor. The term "wireless" referred to tele-communication. Communication between two or more device can be within the short range or may be thousands of kilometers range. Wireless Networks term is refers to a kind of networking that does not require cables to connect with devices during communication [1]. Radio waves are used for transmission at physical level.

The distributed (but wired) sensor network produces local observations using short-range sensors. While the system is temporally continuous, it is spatially sparse, and therefore cannot be used to sense phenomena at a greater resolution than several miles. MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be composed either by mobile nodes or by both fine-tuned and mobile nodes. Nodes are arbitrarily connected with each other and composing arbitrary topology. They can act as both routers and hosts [2]. They have ability to self-configure makes this technology opportune for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is exigently required. In MANET routing protocols for both static and dynamic topology are utilized. To transfer the data between source and destination it follows a routing technique. A mobile host may not be communicate with the destination node directly in a single hop network design, in this view it should occur the multi hop scenario, where the packets can be sent through several nodes which acts as the intermediate between source and destination [3].

Routing protocol specifies how to communicate with the help of routers. It shares information among intermediate nodes then with the whole network. It helps to search shortest route from source to destination. 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 [4]. 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. 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. Selective Packet drop attack is the type of denial of service attack [5].

Packet dropping attack is launched on the forward phase. So it is very complex and difficult to isolate. This attack is very easy to perform but very difficult to detect it. Selfish node also drop packet in their different ways. They drop packets only to save their resources not damage any other nodes. Selective forwarding attacks may damage some mission of applications. Selective Packet drop is only possible when jamming attack is unsuccessful [6]. Once the packet is expected by the compromised node, it can examine the packet headers, categorize the packet, and decide whether to forward it or not. This action is known as misbehaviour. Selective policy known as the Jellyfish attack which is a compromised node that is occasionally drops a small part of consecutive packets and can be efficiently reducing the throughput of a TCP flow to near zero.

II. LITERATURE REVIEW

Pradeep kyasanur et.al proposed in this paper [7] a protocol extension of 802.11 DCF protocol to detect the selfish behavior of the nodes in MANET. The Selfish nodes incomes nodes which select the contentional window (CW) time such that all of its neighbor node cannot able to transmit the packet at the end at it degrade the network performance. The proposed scheme has three mechanisms first one is that the receiver agrees that whether sender is diverting form protocol or not. Second is penalize, in this schema sender is penalize if it is not able to submit the packet to the destination within the time period define in contention window to sender by receiver. The third mechanism is the diagnosis scheme receiver decides whether the sender is selfish or not on the basis of the total data send by the sender and number of times the sender pay plenty.

Yixin Jiangand et.al proposed in this paper [8] a new mutual authentication and key exchange protocol. In the proposed mechanism the identity anonymity and session key renewal are provided. The proposed protocol is based on secrete splitting principle and self-certified scheme. The protocol works in two phases: First phase is the mutual authentication with anonymity when a legitimate user is roaming from the home agent to the visiting agent. The phase uses the temporal identity (TID) rather than the user's real identity. Second phase is the session key renewal phase which renews the shared key which is shared between the legitimate user and the serving agent.

Caimu Tang et.al discusses in this paper [9] a methodology for efficient authentication mechanisms which use by low-power devices. In this mythology only one way single packet transmit by mobile base station for mutual authentication. They used the trust delegation Mechanism by elliptic-curve-crypto system based to generated group pass code for mobile station authentication. By using this authentication mechanism many active and passive attacks will be prevented including the denial of service attack. The mobile device authenticated with the visiting base station only by the exchange of one of the packet. This proposed mechanism is required less computations power and less message exchange delay as compares to other authentication schemes.

Ahmed M.Abd EL-Haleem et.al [10], propose methodology to isolate packet dropping attack by using two disjoint routes protocol in MANET. In this technique two node disjoint routes are selected based in their trust value and use to routes from source to destination. They use DLL-ACK (acknowledgement) and end-to-end Tcp-Ack to identify and examining the behavior of routing path, node. If any malicious node find in the path then path search engine tool get run and identify the malicious node and prevent it.

K. Sangeetha et.al [11] proposed a technique to secure transmission in the MANET using Ad-Hoc on-Demand routing protocol (AODV). Due to lack of resource and infrastructure ad-hoc network is not able to prove logical operation. Proposed scheme is called Enhanced Adaptive Acknowledgement (EAACK) which raises Integrity of IDS (Intrusion Detection System) by using digital signature. It reduces overhead which arise during routing in AODV protocol. In this paper they discuss some previous IDS based technique to identify and remove misbehaving node in network, i) watchdog II) TWOACK(two acknowledgement) III) AACK(end-to-end ACK) IV) S-ACK(secure acknowledgement) V) MRA(Misbehavior report authentication).

Bo Sun Yong et al. [12] proposed in this paper a neighbor set based approach to detect black hole attack and a muting recovery protocol to mitigate the effect of black bole attacks. The demonstrated through simulation that this methods could effectively and efficiently detect black hole attack without introducing much routing control overhead to the network. The data achieved after simulation shows that packet throughput is being improved by at least 15% and the false positive probability is usually less than 1.7%. In the future, they would like to further explore whether there exists a non-cryptography based method to identify them and destination and the optimal detection and response mechanism to improve the packet throughput.

III. RESEARCH METHODOLOGY

Selective packet Drop attack is the partial denial of service attacks which is triggered by the malicious nodes in the network. In the past, many techniques have been proposed to isolate Selective attacks from the network. When this attack is triggered in the network, end to end delay increase as steady rate and throughput of the network reduced. In our work, we work on to detect and isolate Selective Packet Drop attack In AODV Protocol. In the present work we have to apply Diffie-Hellman technique to detect malicious node in the network. First of all a secure channel will be established with the help of Diffie-Hellman technique. After the establishment of the channel, communication begins. Now source sends private key "A" to the source and when destination receive it, also send "B" to the source. When packet reaches to malicious node it does not have key "B". Then this path will not be established due to present of malicious node. Now another path will be choose for communication where there is no malicious node. The secure path will be established after the exchange of the key. In this way packet loss problem due to malicious node will be minimized with the help of Diffie-hellman technique.

As shown in figure 1, the procedure of diffie-helman algorithm is explained in which the source makes the key a, and destination also make the key b. Both the keys are exchanges by the source and destination. When the generated keys are not reached to parties it is analyzed that some intrusion is there in the network.

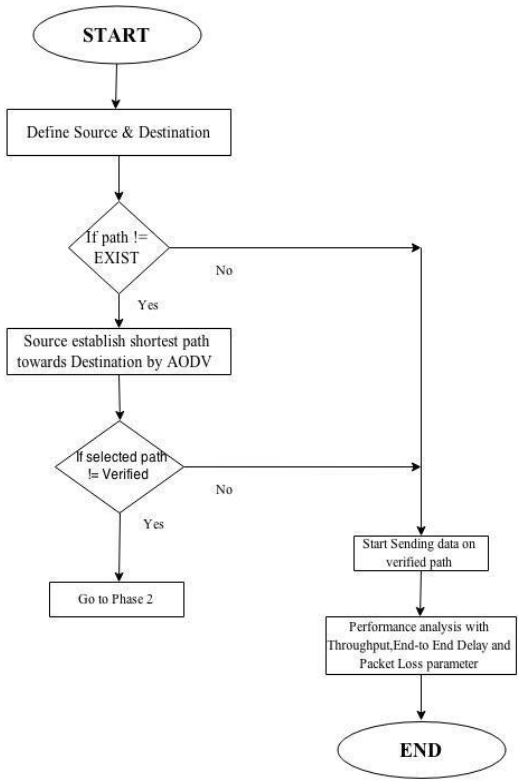

Fig. 1: Flowchart of Diffie-Helman Algorithm

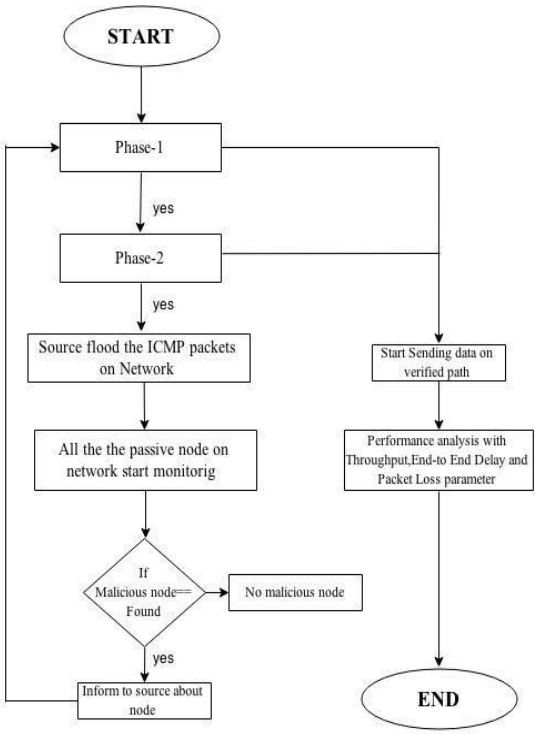

Fig. 2: Isolation Process

As shown in figure 2, the intrusion is detected using the process of diffie-helman. To detect malicious nodes from the network, the ICMP message will be flooded by the source in the network and node which is dropping the packets will be detected as the malicious nodes.

IV. EXPERIMENTAL RESULTS

The proposed method has been implemented in NS2 and the results are analyzed on the basis of various parameters such as delay, jitter, packet loss, and throughput.

- Packet Delivery Ratio

Packet Delivery Ratio = Total Data packets received / Total Data packets sent

- Average End-to-End Delay

Average End to End Delay = ∑ (Time received - Time sent/Total Data packets received

- Packet loss

Packet loss= ∑ (No of packets send – No of packets received)

- Throughput

Throughput = (Total Data packets received/Total Data packets sent)* Time

- Jitter

Jitter = ∑ (Time received - Time sent)

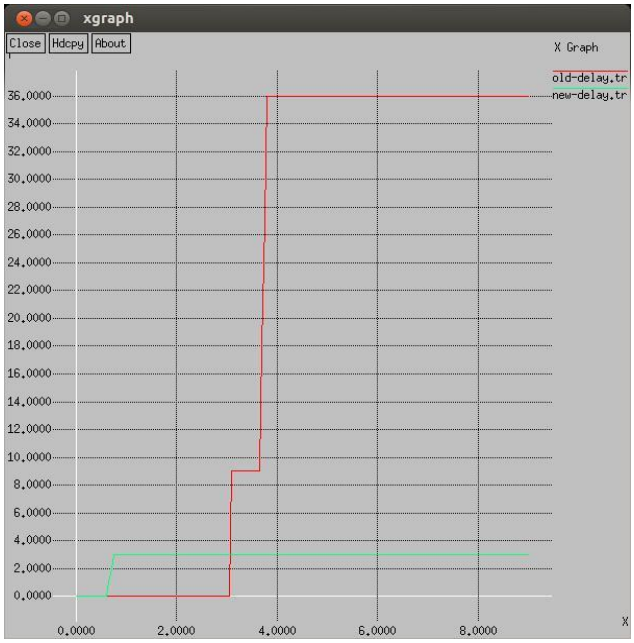

Fig. 3: Delay Comparison

As shown in figure 3, the performance of proposed and existing techniques are compared in terms of delay and it has been analyzed that network delay is reduce in the proposed technique due to isolation of malicious nodes

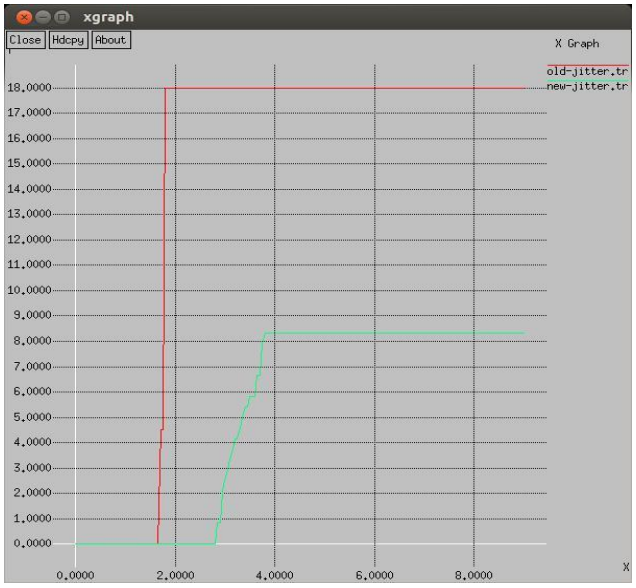

Fig. 4: Jitter Comparison

As shown in figure 4, the network performance is compared in terms of jitter which is per packet delay. Due to isolation of attack the delay in the network is reduce in the proposed technique

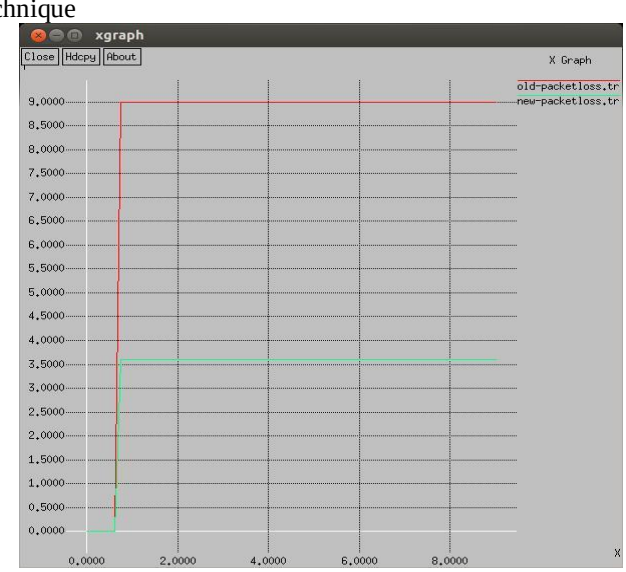

Fig. 5: Packet loss Comparison

As shown in figure 5, the packet loss of the proposed and existing technique is compared and due to isolation of selective forwarding in the network using diffie-helman technique

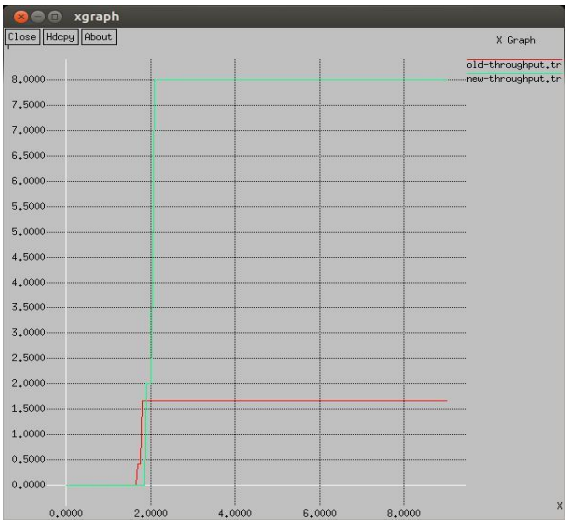

Fig. 6: Throughput Comparison

As shown in the figure 6, the network throughput of proposed and existing technique is compared and it has been analyzed that after isolation of selective forwarding attack throughout is increased at steady rate

Table 1: Throughput Comparison

Node No	Existing Algorithm	Proposed Algorithm
24	2	3
30	4	6
34	8	13

Table 2: Delay Comparison

Node No	Existing Algorithm	Proposed Algorithm
24	180	60
30	220	80
34	260	120

Table 3: Packet Comparison

Node No	Existing Algorithm	Proposed Algorithm
24	8	4
30	12	6
34	14	8

Table 4: Jitter Comparison

Node No	Existing Algorithm	Proposed Algorithm
24	10	7
30	18	12
34	22	14

Table 5: PDR Comparison

Node No	Existing Algorithm	Proposed Algorithm
24	130	60
30	220	80
34	240	90

V. CONCLUSION

In this work, it has been concluded that due to decentralized nature of the network malicious nodes enter the network which are responsible to trigger various type of active and passive attack. The selective forwarding attack is the active type of attack which reduce network performance in terms of various parameters. The novel algorithm has been proposed which is based on diffie-helman algorithm and watchdog techniques. The proposed algorithm is implemented in NS2 and proposed algorithm performs well in terms of jitter, packet loss and throughput.

VI. REFERENCES

[1]. Giovanni Vigna, Sumit Gwalani ,Kavitha Srinivasan, Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool for AODV-based Ad-hoc Wireless Networks", 2004.

[2]. Sevil Sen, John A. Clark, Juan E.Tapiador, "Security Threats in Mobile Ad Hoc Networks", 2010.

[3]. 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, Pages:1035-1043 (2011).

[4]. Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks- A Survey", 2005.

[5]. Gene Tsudik, "Anonymous Location-Aided Routing Protocols for Suspicious MANETs",2010.

[6]. Karim El Defrawy, and Gene Tsudik , "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs" ,IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 9, SEPTEMBER 2011.

[7]. Pradeep kyasanur, "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing, 2005

[8]. Yixin Jiang Chuang Lin, Minghui Shi, Xuemin Shen, "Multiple Key Sharing and Distribution Scheme With (n; t) Threshold for NEMO Group Communications", IEEE 2006

[9]. Caimu Tang, Dapeng Oilver "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE

[10]. Ahmed M.Abd EL-Haleem and Ihab A. Ali, "tridnt: the trust-based routing protocol with controlled degree of node selfishness for manet", IJNSA, Volume-3, No.3, PP.189-203, May 2011.

[11]. [11] K. Sangeetha, "secure data transmission in manets using aodv", IJCCER, Volume-2, Issue 1,PP. 17-22, 1 January 2014

[12]. [12] Bo Sun Yong, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", EPMCC, 2004