ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 6, Issue 4, pp: (181-188), Month: October - December 2018, Available at: www.researchpublish.com

Approach for Secure Channel Establishment to Isolate Selective Forwarding Attack

[1]Gagandeep singh, [2]Arshdeep Singh

[1]Research Scholar, Bhai Gurdas Institute of Engineering and Technology, Sangrur, Punjab, India
[2]Assistant Professor, Bhai Gurdas Institute of Engineering and Technology, Sangrur, Punjab, India

Abstract: **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. 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. 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: **Selective Forwarding Attack, Multi-path Routing, Secure Channel.**

1. INTRODUCTION

A network is a group of two or more computer systems which linked together communication. It is the way of exchange of information to communicate with one another. It is an association or set up of computer devices which are involved with the communication facilities. When numerous devices are joined together to exchange information they establish networks and share resources [1]. Networking is used to replicate, swapping and share information like data communication. Wireless communication is the level at which the transfer of user data over a distance without the use of "wired" or electrical conductor. In this network, each host can transmit data to the wireless node and it does not access pointer controlling medium access. Infrastructure-less networks do not have routers that are fine-tuned. MANET stands for Mobile Ad hoc Network. It is a robust infrastructure-less wireless network [2]. 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. MANET routing protocols for both static and dynamic topology are utilized [3]. To transfer the data between source and destination it follows a routing technique. A mobile host may not 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 act as the intermediate between source and destination. An ad hoc network is a wireless network described by the nonexistence of a centralized and fine-tuned infrastructure. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks [4]. Therefore, we refer to a wireless ad hoc network with mobile nodes as a Mobile Ad Hoc Network. In a MANET, mobile nodes have the capability to accept and route traffic from their intermediate nodes towards the destination, i.e., they can act as both routers and hosts. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes. Routing protocol specifies how to communicate with the help of routers. It shares information among intermediate nodes than with the whole network. It helps to search the shortest route from source to destination. The Proactive protocol contains a fresh list of the route and their destination from the source. In this type of protocol one node contains more than one table for each node in the network. All the nodes are updated regularly [5]. If

the topology frequently changes than update information propagate to every node of the network and update table. Destination Sequence Distance Vector (DSDV) is table-driven routing protocol. It is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements. The sequence number is used to distinguish stale routes from new ones and to avoid the loops formation. Wireless Routing Protocol (WRP) is a routing protocol based on distance vector routing protocol. Reactive Routing Protocol is on-demand a reactive type routing protocol. It is an idle approach in which all the node does not comprise the information of the all the nodes and keeps table only on demand. To find the path route discovery process is followed. Reactive routing protocols are bandwidth effective. In this, routes are built as and when they are required. 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 [6]. The attacker only spoofs the data exchanged in the network without altering it. A passive attack obtains data switched in the network without disturbing the communications operation. The passive attacks are difficult to detection. An active attack is the one in which any data or info is interleaved into the network so that information and procedure may harm. Selective Packet drop attack is the type of denial of service attack. Packet dropping attack is launched in 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 [7]. A Selfish node also drops 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. In these types of attacks, malicious nodes act as normal nodes every time but selectively drop sensitive packets, such as packet coverage the movement of the differing forces. Such selective dropping is tough to detect. Counter measures to selective forwarding attacks cannot recognize malicious nodes nor need time synchronization.

2. LITERATURE REVIEW

Thongchi Chuachan et.al proposed new methodology how to detect and prevent selective packet drop attack. In this paper, they discuss 4 previous methods to protect against these attacks which are reputation based, Acknowledgement based, IDS based and Trusted based [8]. The newly proposed schema called to challenge and response schema. It contains 2 phase I) Key distribution phase II) Challenge ad response phase. The message is encrypted using the public key and routed in two-hop neighbour, take a ratio of local one compare it with the neighbour node. The malicious node can be detected by setting threshold value to cache and at the end this value to the neighbour's value. To simulate this result they use Common Open Research Emulator (CORE).

Seung Yi et.al had discussed some previous mutual authentication schemes of a mobile ad-hoc network. They proposed the symmetric key distribution schemes [9]. They explain PKI (Public key distribution) scheme which based on the symmetric key distribution scheme. In this paper, an author proposed a new authentication scheme named as MOCA which hybrid type of scheme and use both Public key exchange and asymmetric schemes for mutual authentication.

Pradeepkyasanur et.al proposed 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 conventional window (CW) time such that all of its neighbor nodes cannot able to transmit the packet at the end at it degrade the network performance [10]. The proposed scheme has three mechanisms first one is that the receiver agrees that whether a sender is diverting form protocol or not. Second is penalize, in this schema, a sender is penalized if it is not able to submit the packet to the destination within the time period define in contention window to the sender by the 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. If no of plenty paid by the sender is more than the threshold value which is fixed then the sender is selfish and no more data is received from that sender.

YixinJiangand et.al proposed a new mutual authentication and key exchange protocol. In the proposed mechanism, the identity anonymity and session key renewal are given. This protocol provides secure roaming services to the authentic user between the home and visiting agent or in short, this protocol offers secure handoff to the legitimate user [11]. The proposed protocol is based on the secret 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 discussed methodology for efficient authentication mechanisms which use by low-power devices. In this mythology, only one-way single packet transmitted by mobile base station for mutual authentication. They used the trust delegation Mechanism by an elliptic-curve-crypto system based on generated group pass code for mobile station authentication [12]. 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 fewer computations power and less message exchange delay as compares to other authentication schemes.

Ahmed M.Abd EL-Haleem et.al [13], proposed methodology to isolate packet dropping attack by using two disjoint routes protocol in MANET. In this technique, two nodes disjoint routes are selected based on their trust value and use to routes from source to destination. They use DLL-ACK (acknowledgment) and end-to-end Tcp-Ack to identify and examine the behavior of routing path, node. If any malicious node finds in the path then path search engine tool get to run and identify the malicious node and prevent it.

3. RESEARCH METHODOLOGY

We have embedded the Diffie Hellman key exchange algorithm in Bluetooth authentication procedure. In a network, it defines the source node and destination node. To establish the secure channel between communicating parties, each party select a random prime number g and n, selected numbers become public keys of both parties. The source node become master and destination node become a slave, master and slave select their private keys ‘a’, ‘b’ respectively. The master calculates new value “M” from their selected public and private numbers.

$M= g^a \bmod n$

The Slave calculates new value “S” from their selected public and private numbers

$S= g^b \bmod n$

The Master and slave exchange their calculated “M” and “S” values through intermediate nodes. When Slave receives “M” and Master receives "S” both parties will calculate mode inverse value. When master receives value “S” from the slave and calculates new value “K1” from the received “S” value.

$K1=S^a \bmod n$

Slave receives value “M” from master and calculates new value”K2” from the received “M”

$K2=M^b \bmod n$

After calculating “K1” and “K2”, both parties establish a secure channel, by calculated new key “K”. If both communicating parties have same “K1” and “K2” values, a secure channel is established between Master and Slave.

K=K1+K2

When the secure channel is established between master and slave, communication starts between both parties. The communication between Master and Slave is encrypted with public keys. Each party uses their own private keys to decrypt the communication. The following flowchart explains the above work, how the embedded Diffie-Hellman works in the network. 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 receives it, also send “B” to the source. When a packet reaches to the malicious node it does not have key “B”. Then this path will not be established due to present of a malicious node. Now another path will be chosen 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.

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 6, Issue 4, pp: (181-188), Month: October - December 2018, Available at: www.researchpublish.com

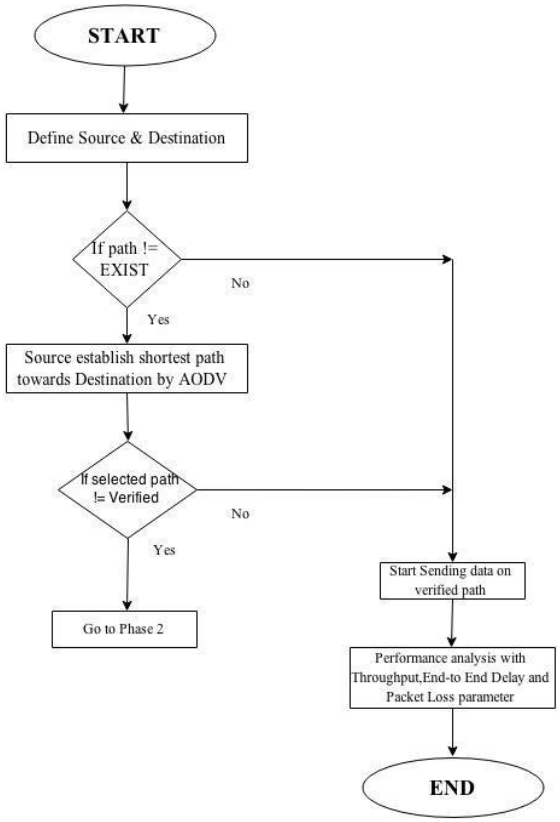

Figure 1: Flowchart of Proposed work part I

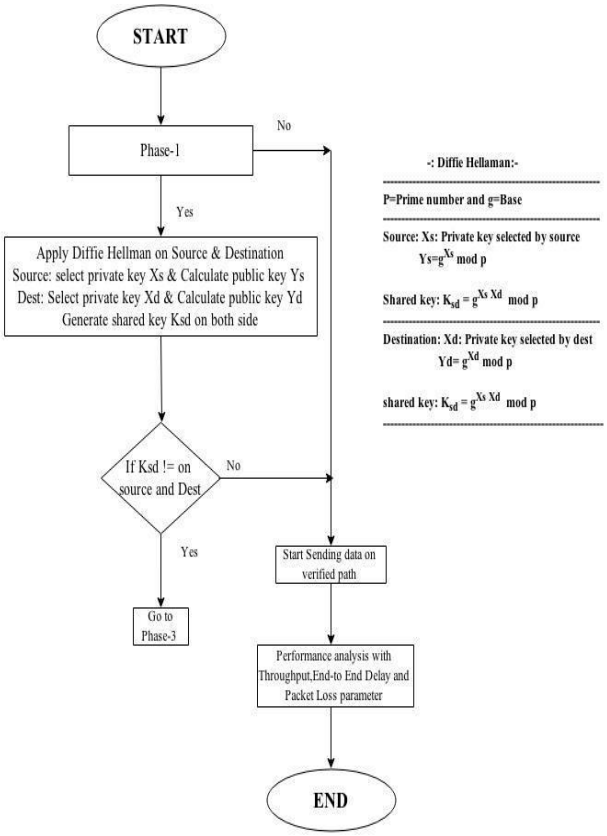

Figure 2: Flowchart of Proposed work part II

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 6, Issue 4, pp: (181-188), Month: October - December 2018, Available at: www.researchpublish.com

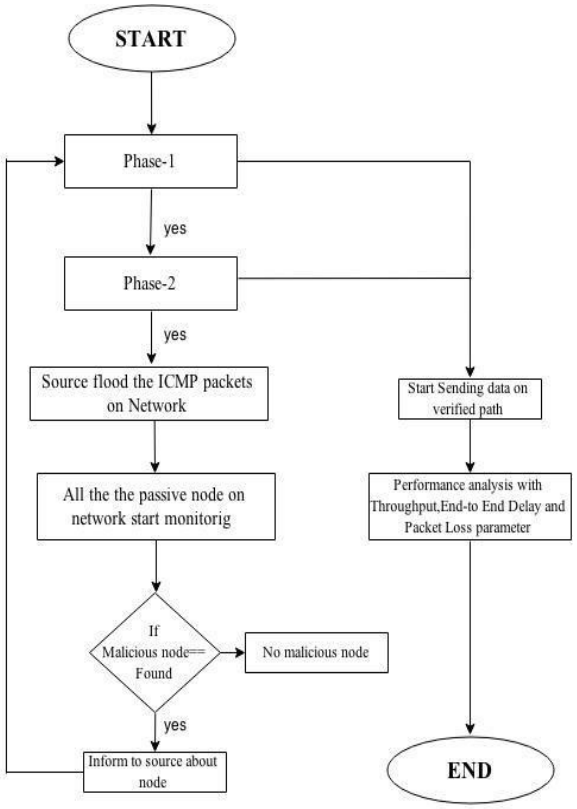

Figure 3: Flowchart of Proposed work part III

Experimental Results

The proposed work is implemented in NS2 and the results are evaluated by making comparisons against proposed and existing techniques in terms of several parameters.

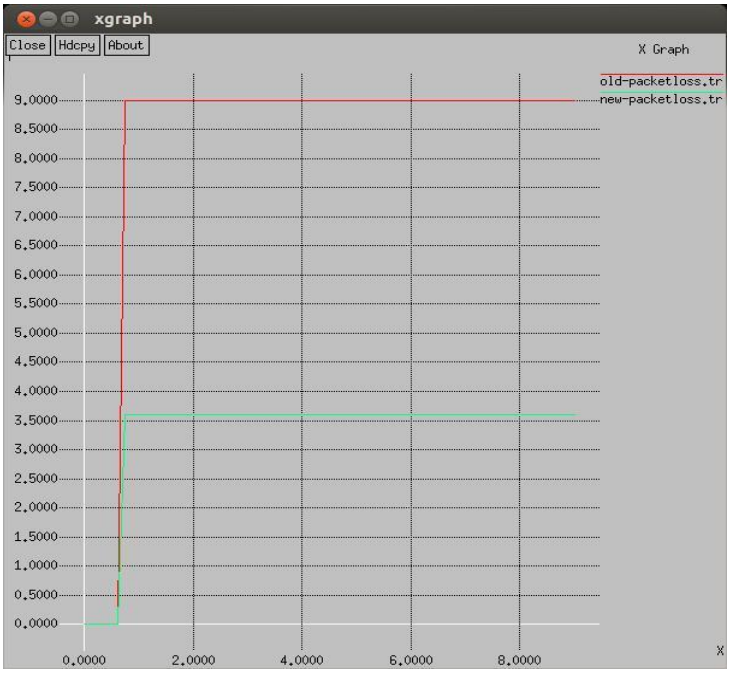

Figure 4: Packet loss Comparison

As shown in figure 4, the packet loss of the proposed and existing technique is compared and due to an isolation of selective forwarding in the network using the Diffie-hellman technique.

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 6, Issue 4, pp: (181-188), Month: October - December 2018, Available at: www.researchpublish.com

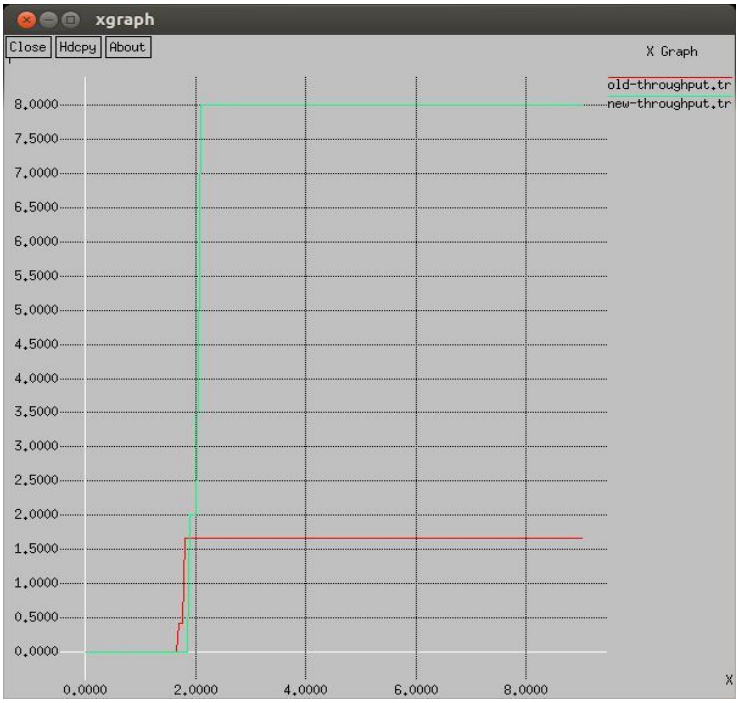

Figure 5: Throughput Comparison

As shown in figure 5, 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 a steady rate.

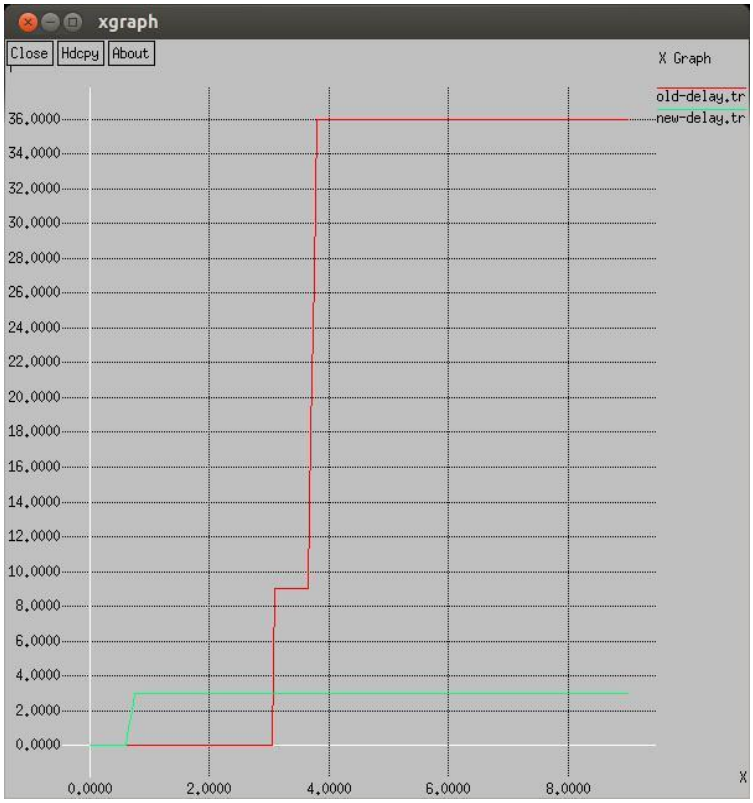

Figure 6: Delay Comparison

As shown in figure 6, the performances of proposed and existing techniques are compared in terms of delay and it has been analyzed that network delay is reduced in the proposed technique due to an isolation of malicious nodes.

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 6, Issue 4, pp: (181-188), Month: October - December 2018, Available at: www.researchpublish.com

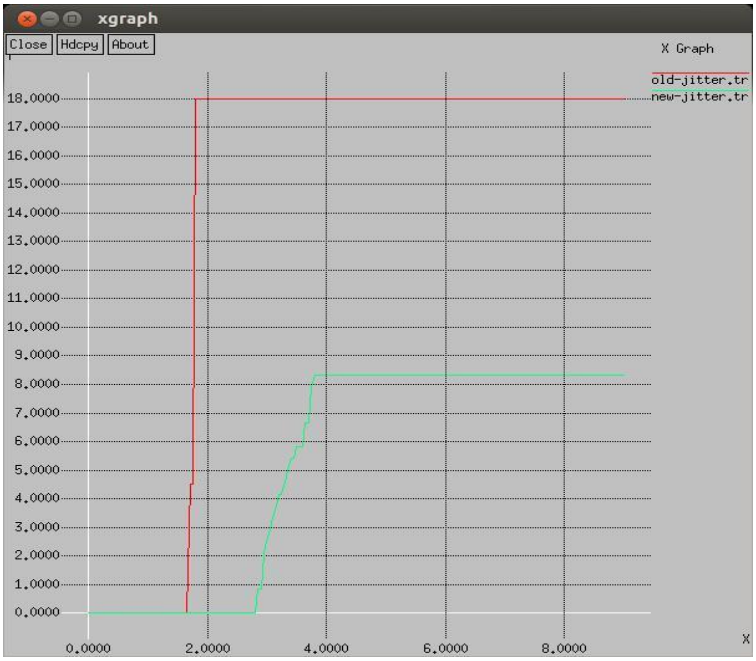

Figure 7: Jitter Comparison

As shown in figure 7, the network performance is compared in terms of jitter which is per packet delay. Due to an isolation of attack, the delay in the network is reduced in the proposed technique.

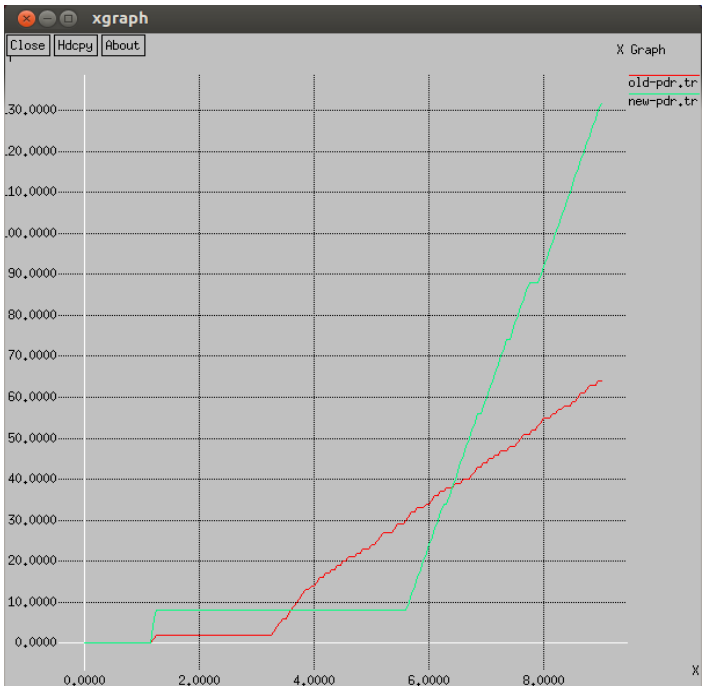

Figure 8: PDR Comparison

As shown in figure 8, packet delivery ratio is increased after the removal of malicious node from the given network.

4. 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 reduces 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.

REFERENCES

[1] Thongchi Chuachan and Somnuk Puangpronpitag ,"A Noveel Challebge & Response Scheme Agaist Selective Forwarding Attacks in MANET", IEEE, 2013

[2] Seung Yi, Robin Kravets,"Key Management for Heterogeneous Ad Hoc Wireless Networks",10th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648

[3] Pradeepkyasanur,"Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing,2005

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

[5] CaimuTang ,DapengOilver "An Efficient Mobile Authentication Scheme for Wireless Networks",IEEE.

[6] 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.

[7] Sunil Taneja, Dr. Ashwani Kush and Amandeep Makkar, "End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011.

[8] Andul Haimid, Bashir Mohamed, "ANALYSIS AND SIMULATION OF WIRELESS AD-HOC NETWORK ROUTING PROTOCOLS"2004.

[9] GiovanniVigna, SumitGwalani ,KavithaSrinivasan ,Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool for AODV-based Ad-hoc Wireless Networks", 2004.

[10] SevilSen, John A.Clark, Juan E.Tapiador,"Security Threats in Mobile Ad Hoc Networks", 2010.

[11] RushaNandy, "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).

[12] Wenjia Li and AnupamJoshi,"Security Issues in Mobile Ad Hoc Networks- A Survey",2005.

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