ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

KEAM- To Isolate and Prevent Selective Packet Drop Attack in MANET

Sagar Babubhai Patolia[1], Narendra Kumar Bagde[2]

P.G. Student, Department of Computer Engineering, Lovely Professional University, Phagwara, Punjab, India[1]

Associate Professor, Department of Computer Engineering, Lovely Professional University, Phagwara, Punjab India[2]

ABSTRACT:A Selective packet drop attack is notorious security problem in wireless Mobile Ad-Hoc network (MANET). A mobile Ad-Hoc network is wireless networks without any pre-existing infrastructure and centralizes control. They have self-organizing capabilities with mobile nodes. Ad-Hoc network contains multi-hop routes capabilities within short transmission range. Because of openness nature MANET is malicious by attacker. Several approaches have been proposed for finding malicious activity in MANETs. Due to nonexistence of MANETs infrastructure and well defied perimeter MANETs are susceptible to variety of attacker types. To develop a mechanism which provide strong security and understand the malicious node activity in the MANETs. A new mechanism presented is called **KEAM (Key Exchange and Monitoring),** which isolate malicious node on selective path in AODV routing protocol and secure the channel. This new methodology is named as "Isolate and prevent Selective Packet Drop Attack in MANETs. It is based on Diffie-Hellman Key exchange and monitor mode technique. Experimental result will be drone with use of NS-2 simulator and simulate result for Throughput, Packet loss, End-to-End Delay and compare the result with existing technique.

KEYWORDS: MANET, AODV, ATTACKs :Selective packet drop, Diffiehellman, Monitor Mode

I. INTRODUCTION

To increase the wireless reachability, mobile Ad-Hoc Networks(MANETs) are required to relay data packets through multiple devices. A mobile Ad-hoc network is distributed, self-configuring and self-administrating highly dynamic wireless environment. Each node consuming features like self-governing, limited battery power and distributed multi-hop environment. Mobility and unreliable wireless channels are the result of an unpredictable-dynamic network topology. Such a network is helpful in creating communication between MANET nodes that are outside the wireless transmission range. Due to fully distributed characteristics it is not feasible to establishing centralized node which can collect all the network traffic.

Such type of dynamic networks are more susceptible to attack than compared to wired network. This is because of the following reason:

a) Openness of medium
b) Dynamically changing network topology
c) Cooperative Algorithm
d) Lack of Centralized Network topology
e) Lack of clear line of defence

The main objective in this paper is to isolate and prevent selective packet drop attack from routing path in AODV routing protocol of MANET. MANETs are typically challenged with a large number of the network vulnerabilities. In general, MANET nodes are usually assumed to be a trustworthy and cooperative. Unfortunately, users in MANETs have a tendency to drop the other's packets to terminate a data communication, known as a packet drop attack. To impersonate as a normal node, an attacker pretends to be a normal one, and does not forcibly acquire a routing path. To terminate the communication, the attacker discards to forward data packets for a receiver.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Several results have been proposed to protect the selective packet drop attack, and can be classified into four main categories, namely reputation-based [17,18], acknowledgement-based [19,20], IDS-based [21-24] and trusted base [25-27].Even though all these proposed schemes have been proposed, MANET environment is still vulnerable to the attacking method. So, we have designed a new scheme to locate and identify attacker nodes. In this paper, we propose a key exchange scheme to detect a selective forwarding attack in MANETs. A proposed scheme contains two phases. The first one is a key exchange phase. The second one is a monitor node phase. In both stages, we assume that MANET nodes can use channels to transmit routing messages. An attacker can be detected by monitoring the channel with request response schema.

The major threats which Breach security in wirealess network authentication , non-repudiation, availability, integrity, confidentiality.

A) **Authentication and non repudiation**: Authentication allow node to verify identity of next node with which it is commuincating. Non-repudiation is provethat legitimate sender sent a message[1].

B**) Passive Vs. Active Attacks**: Passive attacks are launch to release or lose confidentiality of valuable information in networks.In this type of attack , attacker not harm the system and its resources. Eg. evasdroping. Active attack are made intentionaly either change or delete confidential information fro disturbing the normal functioning o fnetwork. Eg. Falsse message propogating attack, man-in-middle attack[1].

C) **Internal Attack** :Internal attack are compromised of node that are part of the path which being use for sending the data.In this attack malicious node gain unothorised access on the path and pretend to be genuine node.traffic can be watched between other nodes and may participate in the activities of other networks.

D) **External Attack** : The external attack is conceded out by the nodes which do not belong to network. It may cause unavalibility and congetion by sending unvaluable and arbage information for the network jamming.

E) **Black-hole attack** : In blcak hole attack malicious node use its routing protocol to know other node that it has shortest path towards destinationand attacker drop the packet to reduce the quantity of information is available to other node. This type of attack made intentionaly for deniall of service type attack[9]. This make destination system unreachable or shutdown in network.

F) **The worm Hole Attack**: The worm hole attack is quite tipical and merciless attacks, which can be executed in MAnET. In this type of attack message is captured from the one region of network and replaying in other region. Attacker creates tunnel between two node which participate for communication. One attacker gather all message and other attacker replay to misinterprate to make destination unrechable from network.

The remaining paper is organized as follows. Section II discusses the background and related work. In section III we describe the Routing IN MANETs. Section IV presents Selective packet drop attack. Section V shows the research objectives .Section VI Proposed Design. section VII gives the conclusions and the future work.

II. BACKGROUND AND RELATED WORK

For reputation based schemes, MANET nodes normally collect sets of the traffic behaviours, and provide detection mechanisms. The schemes mainly rely on routing and data forwarding behaviours.For example, Akbani et al. have proposed EMLTrust [18], and used Machine Learning (ML) methods to sense malicious behaviors. Dini et al. have proposed a scheme, called RCAR [17] to detect and avoid attackers. The RCAR functionalities actively force MANET users to forward data messages for former users. However, both EMLTrust and RCAR suffer from a high delay for classification period, and low detection accuracies.

For acknowledgement-based schemes, TWOACK [19] and NACK [20] have been proposed by Balakrishnan et al. and Sun et al. respectively. In TWOACK, misbehaving nodes have been alleviated by using a special acknowledgement packet. There are at least three sequential intermediate nodes to complete operations. Suppose N1, N2 and N3 are intermediary nodes. N1 forward data messages to a destination. The data messages are then passed through N2 to N3. Finally, N1 waits for acknowledgements from N3. For an acknowledgement, N1 notifies N2 as a normal node if N1 can receive the acknowledgement from N3. For NACK, the protocol has been extended fromTWOACK. NACK routing messages have been confirmed using Certificate Authority (CA). A timestamp

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

comparison is also deployed to shrink the acknowledgement flood in NACK. There are some ineffective points of TWOACK and
NACK. The TWOACK rises network overhead due to the excessive acknowledgements. In addition, the TWOACK notices entire links as misbehaving nodes if a selective attacking method has been found. For NACK, CA offline installation is not suitable in several MANET environments.

IDS-based schemes are primary security approaches. MANET researchers have widely used IDS to detect numerous MANET attacking methods, including the selective forwarding attack. The researchers incorporate IDS into their detection systems, and increase the truthfulness by using a wide range of methods (such as machine learning techniques). IDS can properly return a number of accuracy ratios. However, IDS requires heavily computational power to analyse the attacks. In addition, IDS is assumed to be always on that is probably not suitable to use in several MANET Environments. Several trust-based schemes [25-27] have been proposed to enhance MANET routing securities from various types of attacks, including the selective forwarding attack. The schemes evaluate the reliability of the next hop using fuzzy logic and other algorithms. However, the parameters of the algorithms can be very sensitive to the results. In particular, unpredictable MANET characteristics can cause inaccuracies. So, the effectiveness of the trust-based schemes to protect against the selective forwarding attack is still questionable.

Thongchi Chuachan and Somnuk Puangpronpitag et al. [10], proposed new methodology how to detect and prevent selective packet drop attack. In this paper they discuss 4 previous method to protect against 1.reputation bsed 2. Acknowledgement based 3. IDS based 4. Trusted based. The new proposed schema called challenge and response schema. It contain 2 phase I) Key distribution phase II) Challenge ad response phase . The message is encrypted using the public key and routed in two-hop neighbor, take ratio of local one compare it with neighbor node.The melocious node can be detect by setting thresold vlaue to cache and at the end this value to the nieighbours value. To simuate this result they use Commn Open Reserch Emulator (CORE).

Hung-Min Sun and Chiung-Hsun Chen and Yu-Fang Ku et al.[11], they propose an acknowledgment-based technique, called NACK, to detect and mitigate the dropping attacks. Moreover, NACK can resist the collusion attack by using the timestamp mechanism. Although NACK can resist successfully collusion attack, it only considers the case of two consecutive nodes.

DjamelDjenouri and NadjibBadache et al.[12],propose a new solution to monitor, detect, and safely isolate such misbehaving nodes, structured around five modules: (i) The monitor, responsible for controlling the forwarding of packets, (ii) the detector, which is in charge of detecting the misbehaving of monitored nodes, (iii) the isolator, basically responsible for isolating misbehaving nodes detected by the detector, (iv) the investigator, which investigates accusations before testifying when the node has not enough experience with the accused, and (v) finally the witness module that responds to witness requests of the isolator. These modules are based on new approaches, aiming at improving the efficiency in detecting and isolating misbehaving nodes with a minimum overhead. They also mathematically analyze their solution and assess its performance by simulation, and compare it with the watchdog, which is a monitoring technique employed by almost all the current solutions.

III.ROUTING IN MANET

The routing in a MANET is intrinsically different from traditional (current) routing found on centralized structured networks. Routing in MANET depends on many factor including Route initiation , Topology selection of routers that all could give heuristic approch toward finding the path correctly accurately and efficently.

By this characteeristics MANET protocol classified as proactive(Table-Driven) or Reactive(On-Demand) routing protocol [2]. Proactive routing protocol is also known as Table-driven protocol it self described that it keeps tracks of all the route information towards source to destination.All the route information hop by hop stored in Tablewhich use by each node to forward data to destination when path is undefined. Eg. DSDV, Fishey state, WRP. While Reactive

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

routing protocol known as On-Demand as per its characteristics. Node establish route when it required to flood packet so it is called as On-Demand or lazy protocol.This protocol named as source intiated because when source wants routes to destination it initiates route discovery. It maintain consistent up-to-date routinf information from each node to every node in network

1)AODV [Ad-Hoc On-Demand Distance Vector][5]:

Ad-Hoc is combination of relative and distance vector mythology designed for woreless ad-hoc netweorks. When source want to forward packet it initiates route discovery procwss. Source node (S) flood RREQ (rout request) to setup route to destination (D).When intermedate node receive RREQ it update its route table for reverse path towards source. The RREP(route repaly) is sent back to source when RREQ is reach to destination or intermedatory node that has current route to destiantion. In AODV sequence number is used to determine current (resh) route information and to prevent loop in route. In case of multiple routes with intermediate node select route with highest sequencenumber and shortest hop-count to send packet. When link get failure route error packet will be generated and send back to source and generate new route.

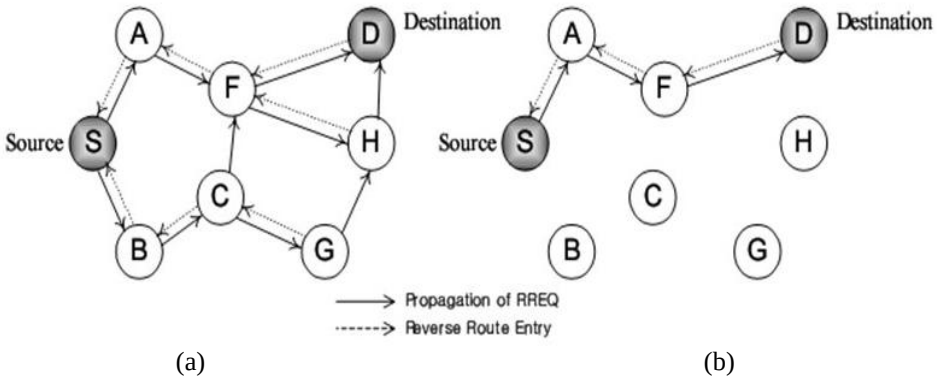


Fig.1. (a) RREQ Braodcast (b) RREP Forwardpath (Route Determination From Source to Destination)

2) DSR [Dynamic Source Routing][6]:

DSR is reactive type of protocol.The indentical features of DSR is source routing in which all mobile node maintain route cashes that preserve the source routes of which all mobile node know (aware). All caches updates for new learned routes 2 Major phase. I] Route Discovery II] Route Maintenance
In DSR when On-Demand route reqquirement comes first it willl check route caches for preevious route information to destionation. If trhe previous route link is expire then route discovery is establish and forward new RREQ. Route maintenance is accomplished when route error and acknowledgement came for fatal transmission problem.

IV. SELECTIVE PACKET DROP ATTACK

Once the packet is expected by the compromised node, it canexamine the packet headers, classify the packet, and decidewhether to forward it or not. This action is known asmisbehaviour.Selective Packet drop is only possible when Jamming attack is unsuccessful.Packet drop attack is some what releated to black-hole attack but it hard to detect and prevent it.In this attack, nodes in path suppose to forward the packet towards destination but malicious node discard the some amount of packet to disrupt the network[10].The melicious node can succeed this attack selectively so it is callled selected packet drop attack.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

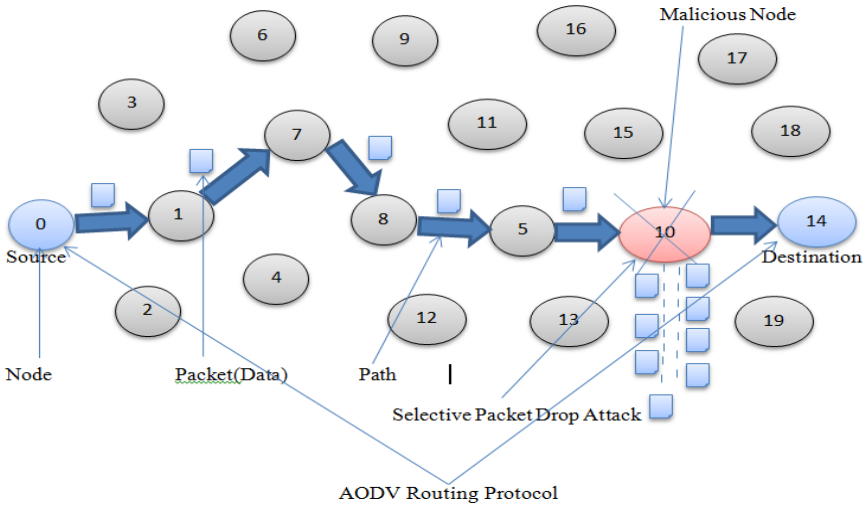


Fig 2: Packet Drop Attack

By dropping packet for selected destination of certain time of day, a packet every "n "packet of every "T" second or randomly selected portion of packet. To avoid selective packet drop attack most powerful technique is to observe the behaviour of traffic in route set the threshold, calculate the reverse path from any point in route and identify the melodious node and it use the key distribution technique (KDAM) to secure routing and it will provide the confidentiality that the legitimate source send these packet.

V. RESEARCH OBJECTIVES

Following are the various objectives of this research work:

The study focus on analysis of Selective packet Drop attack in MANET and its consequences.To study the previously proposed plans suggested for counter measurement of Selective Packet Attack. The aim of the study to detect the Selective Packet Drop in MANET using AODV protocol.Analysing the effects of Selective Packet drop attack in the light of Packet loss, throughput and end-to-end delay in MANET.To propose new scheme to detect malicious nodes in the network which are responsible for triggering the Selective packet Drop attack in the Network.Simulating the detection of Selective packet Drop attack using AODV protocol in MANET using NS-2 tool.

VI. PROPOSED DESIGN

A. Schema Description

Proposed technique is to detect packet drop attack in MANET and improve the performance of the network. The concept use in the proposed technique is based on the monitoring mode and key exchange technique. Our challenging schema is work in 2 parts. (I) Key exchange and (II) Monitoring mode technique.

B. Key Exchange:

Ad-Hoc network is created with finite number of nodes. Select the source and destination from the given node. Then check for the availability for the path between node. If path does not exist between the node then called the AODV routing protocol and deploy the shortest path between the nodes. The node who participates in routing willbecome a active node. Now start to flood the packet from the source to destination. The attacker on the path who selectively drop the packets and result will be the packet loss in the given network. To detect this malicious node first we have to make the channel secure so the result will be no interruption in the communication.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

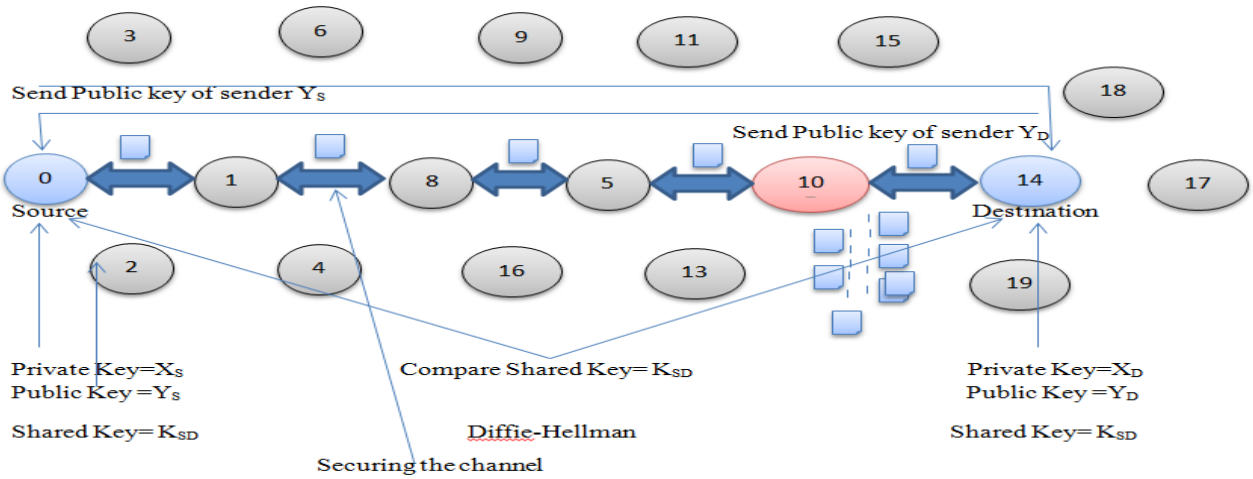
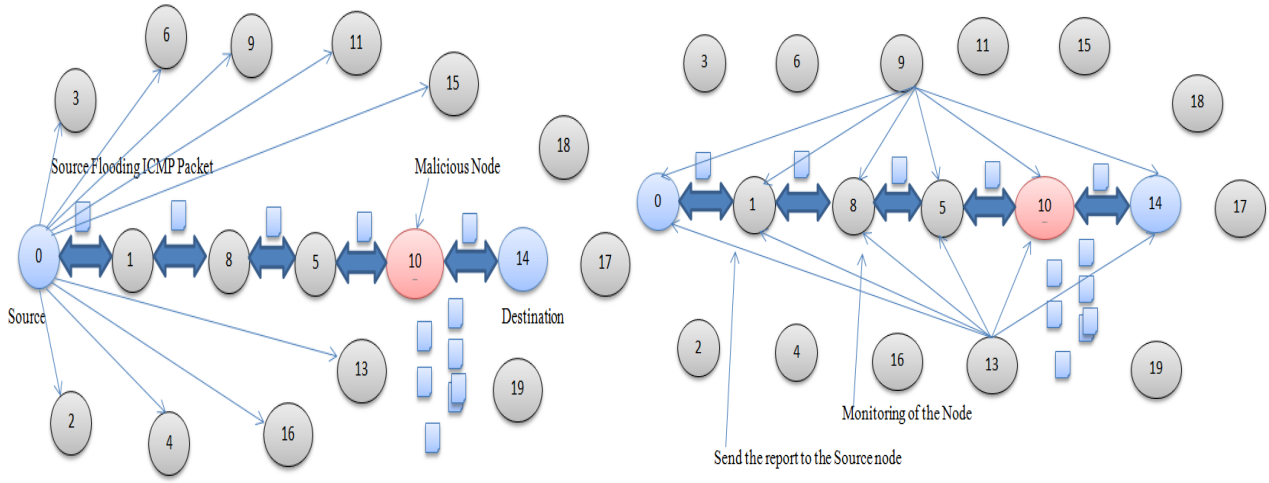


Fig 3: Key Distribution Phase

Fig 3 shows that We apply the Diffie -Hellman algorithm on both sender and receiver to make channel secure. First sender and receiver generate prime number (p) and base (g). Now sender generate its private key **Xs** and calculate it public key **Ys** with use of formula: **Ys= g^{Xa} mod p**. now sender share its public key, prime number and base key to destination node. On Destination it generate its private key Xd and calculate its public key Yd= g^{Xd} mod p. Now source and destination share its public key to source. No both side generate share key with the formula: Ksd= g^{XsXd} mod p. Now sender and receiver match their shared key if it match then sender continue the communication towards the destination. If the shared key does not match then source flood the ICMP message in the network and call the monitor mode technique which is shown in fig 4.



(a) (b)

Fig 4: (a) ICMP Flooding (b)Detection of malicious node

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

C. **Misbehavior Detection**

Monitor Mode:when the source flood the ICMP packet all the node in the network apart from node who are participated in the routing become a passive node. All this passive node starts monitoring to one hop node , which is use for routing. Each monitoring node send request to node which is on path. If the replay didn't comes in particular time stamp it considered as malicious node and all the information about malicious node is send to the Source node. Source node alert its as malicious and start to deploy the new path towards destination and secure it by deffiee-hellman.

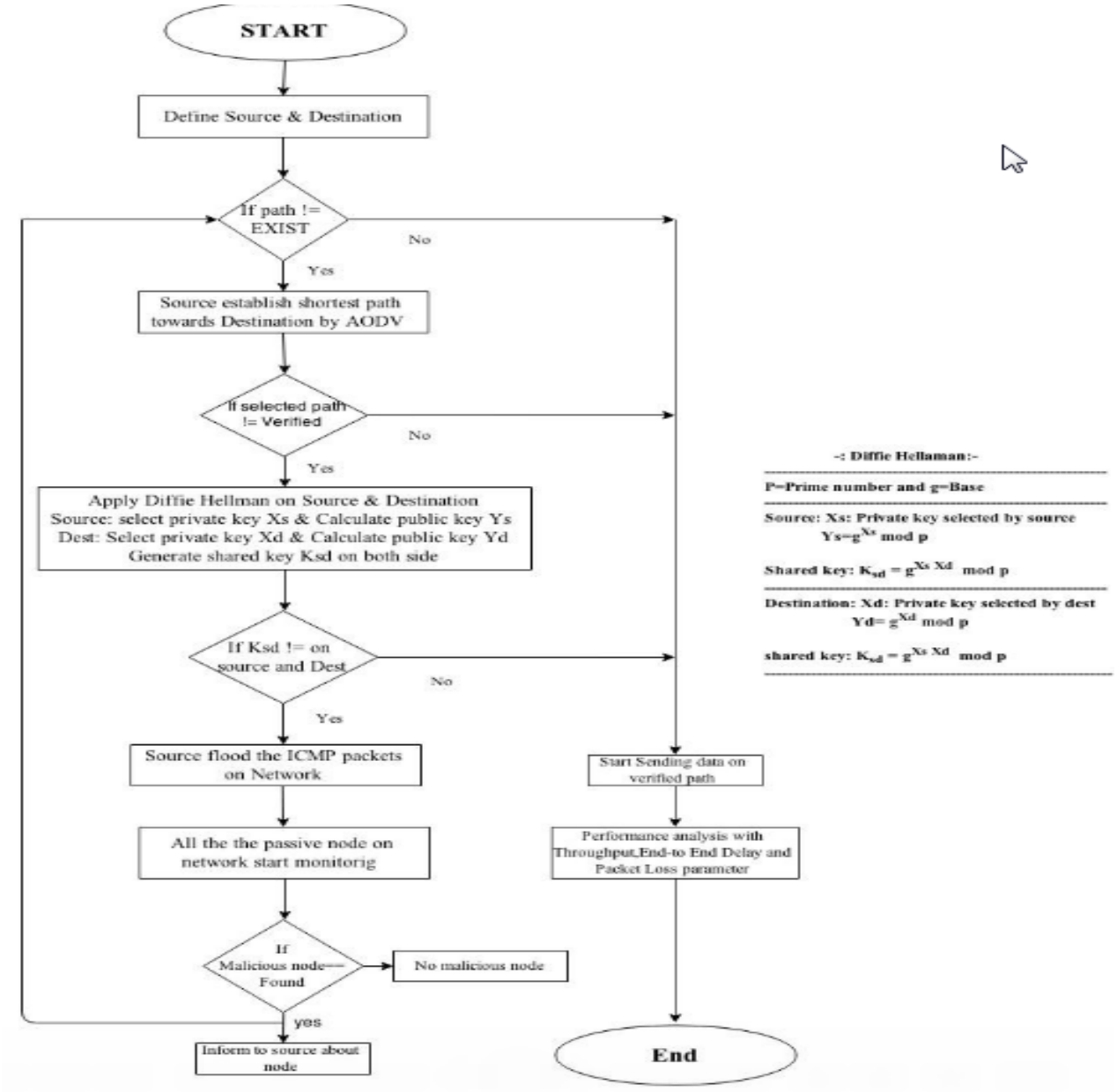


Fig 5 : Flow chart

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

VII. PERFORMANCE EVALUATION

❖ **Simulation Configuration:**

Our Simulation is conducted within the network Simulator(NS) 2.35 environment on platform with GCC 4.3.4 and Ubuntu 14.04.1. In NS 2.35.we make configuration with 23 nodes and flat grid size of 800x800m.

❖ Simulation is being done by AODV routing. We generate the result in NS-2 with use of reference node technique. The graphs are used to signify the variation in throughput and end-to-end delay using the proposed method. Green line characterizes the change in case of the new scenario and red colour represents the conventional method. These two parameters are a widely used for validating the confirming the use of particular methods. Throughput can be defined as the number of packet data received per unit time whereas end-to-end delay defined as the time taken between sending of a packet and it's receiving on the destination.

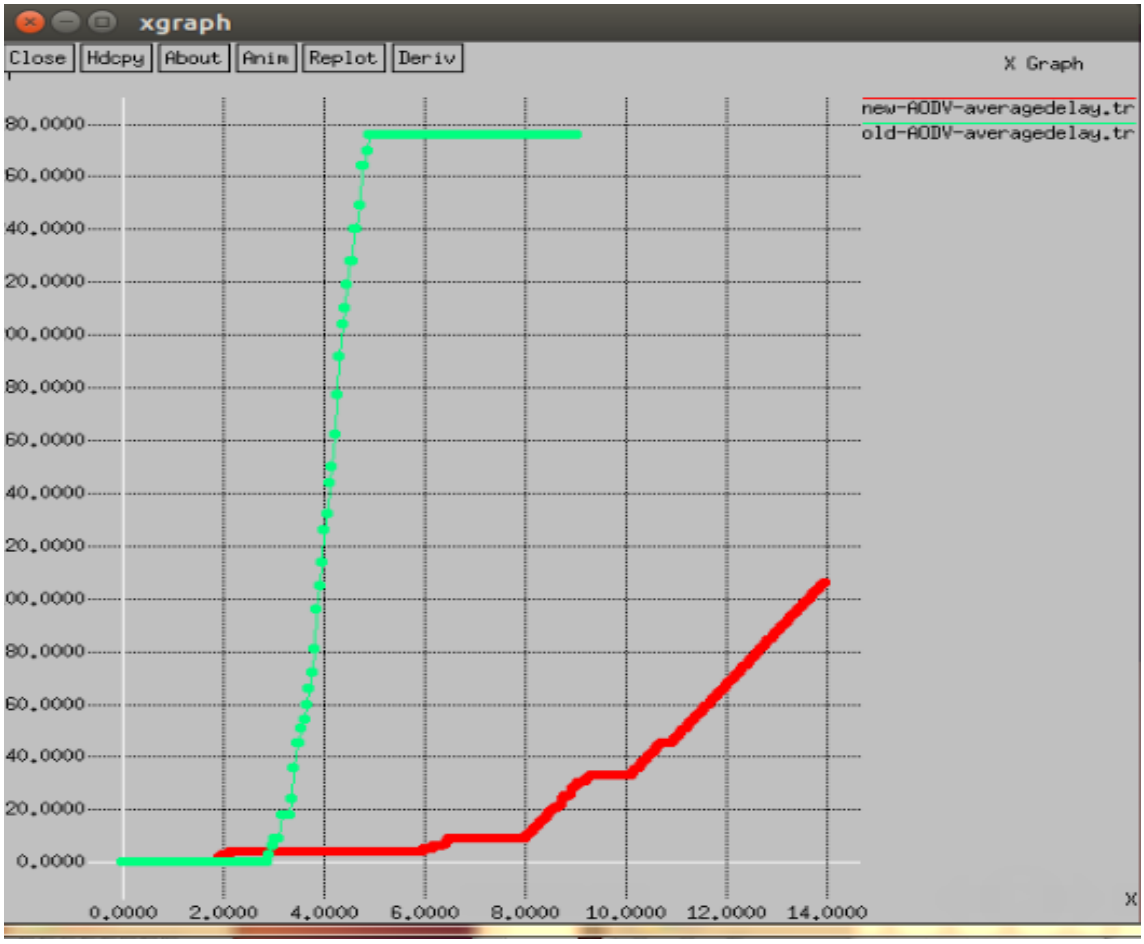


Fig 6: Average End-to-End Delay

Figure 6.Shows the change in end-to end delay after deployment of the proposed method. It shows that our proposed KEAM schema reduce 90% of end-to-end delay while packet is going to transmit from source to destination In the previous schema, the delay starts linearly increasing when there is presence of malicious node in the path mark as green line whereas in absence of malicious node delay first decrease but the new path deploy because of malicious activity it

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

will be not as much shortest then previous so at some point of time the peak of the graph increase and decrease because of delay which mark as red line in graph.

Fig 7.Represents the average throughput after applying proposed method. As delay in the network is minimum because of isolation of malicious node, so throughput of the network is linearly increased after some pint of time. From graph we can see that when number of packet increase throughput is gradually increase with time in our proposed schema shown by red line. While green line represents previous schema when the malicious node present in the network at that time packet continuous drop so the line is constant for some period of time.

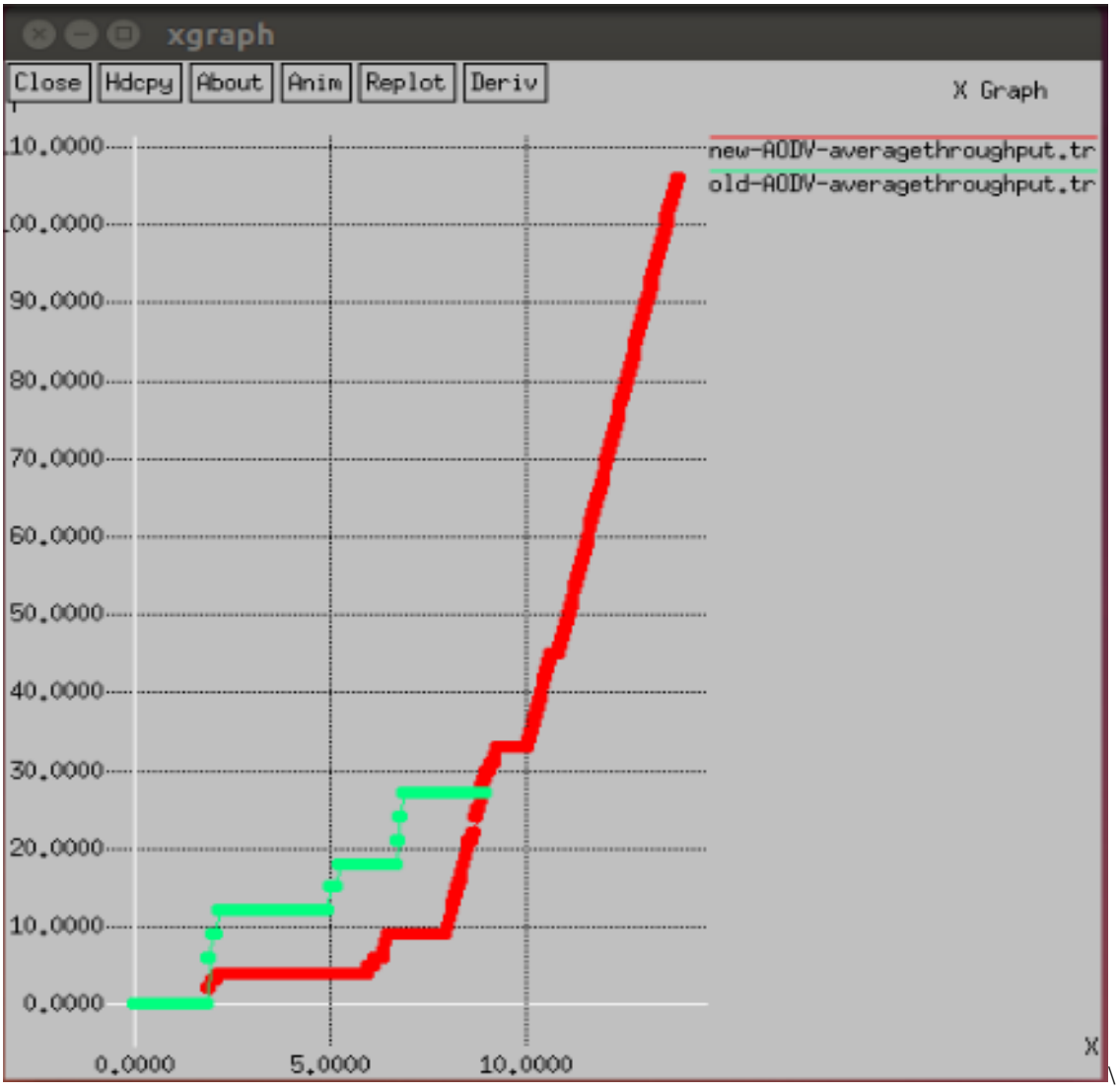


Fig 7: Average Throughput

Calculating the Throughput of the network , we have used the following formula:
Throughput = Packet received * 8/ Amount of packet forwarded (over some point of time).

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

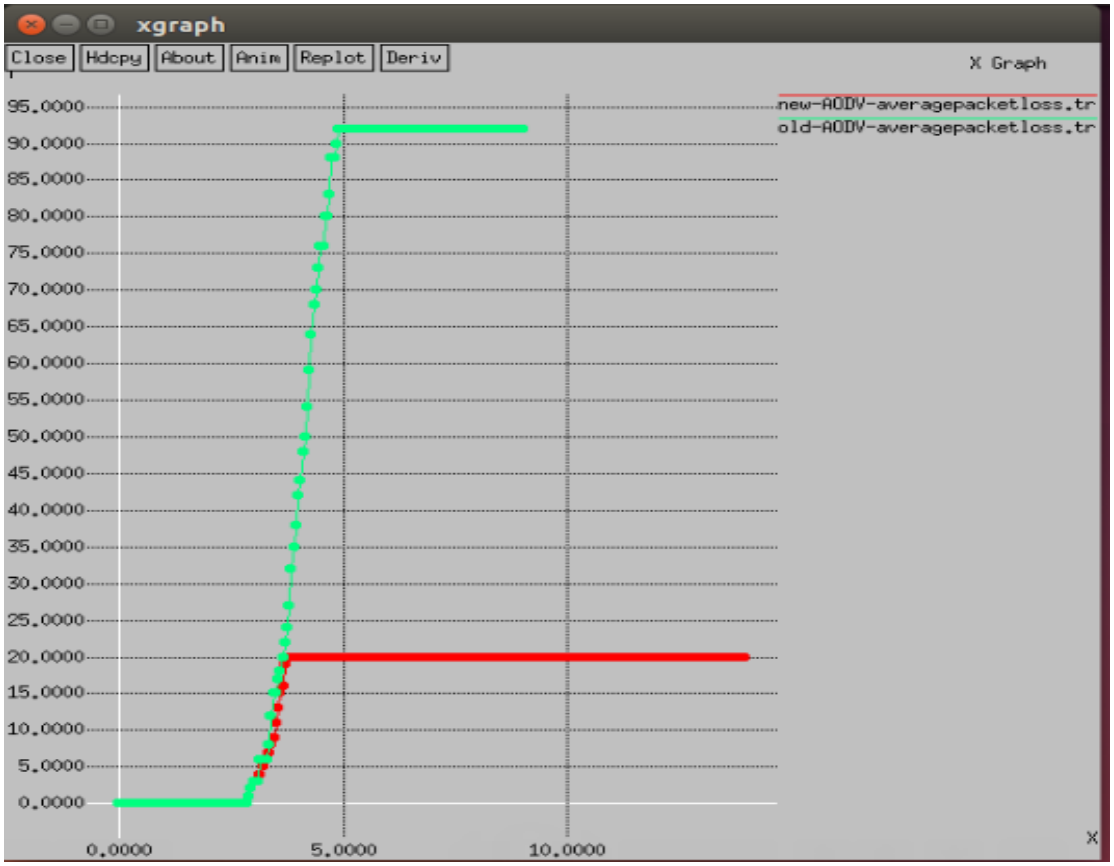


Fig 8 : Average Packet loss

As we have applied the Diffie-hellman and monitoring algorithm for setting up the path then packet loss is less as compared to the previous scenario. We make the channel secure so final result comes is maximization of throughput and minimization of packet loss. In previous schema malicious node continuously dropping the packet so final output is major loss of packet. In fig 8: we see that the green line is continuously increase because of dropping of the packet and red line constant after some time because of securing of channel. We reduce the 80% of the packet loss by applying KEAM technique.

VIII. FUTURE WORK AND CONCLUSION

Mobile ad-hoc network have been wast area of research work from past few years because it's widely used application in battlefield and business purpose. Due to openness and dynamic topology network is vulnerable from attacker.In this paper we proposed and evaluated two network layer schema Key Exchange and Monitor node-KEAM , which can easily deploy to source initiated routing protocol such as AODV. The schema detects the malicious node from routing path in network so when new route establish it would be free from malicious activity and the result improvement in the packet delivery ratio and minimize the end-to-end delay .Simulation show that monitor node technique easily detecting the misbehaving node and increase 80% throughput in network.

We would continue our future work in the following direction: Make further improvement in the acknowledgement and key exchange model posted in this report and take other decision factor for our model. Comprehensive performance evaluation will be conducted in the light of multiple packet drop attack.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

REFERENCES

[1] W.Stallings," Network Security Essentials: Application and astandards", 2nd Edition, prentice Hall ,Upper Saddle River,2003.
[2] C-K Toh,"Ad Hoc Mobile Wireless Networks",PEARSON,2013
[3] S. Corson, "Mobile Ad Hoc Networking: Routing Protocol Performance Issues and Evaluation Considerations" .IETF, RFC 2501, January 1999.
[4] Ramna,K.S., Chari, A.A., &Kasiviswanth,"A survey on trust management for mobile ad hoc networks. International Journal of Network Security & Its Application ,"(IJNSA), 2(2),PP.75-85,2010.
[5] C. Perkins, E.Belding-Royer, and S.Das, " Ad Hoc On-Demand Distance Vector(AODV) Routing",IETF, RFC 3561, July 2003.
[6] D. Johnson, D. Maltz, Y-C.Hu, J.Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks(DSR)", Internet-Draft, February 2002.
[7] B.Wu, J.Chen, M.Cardei," A survey on Attacks and Counter measures in Mobile Ad Hoc Networks," Wireless Network Security,PP. 103-135,2007
[8] Dongbin Wang, Mingzeng Hu, Hui Zhi,"A Survey of Secure Routing in Ad Hoc Networks",The ninth International Conference on web-age Information Management, pp.482-486,2008.
[9] I.Aad, W.E. Knightly,"Impact if Denial of Service Attacks on Ad-Hoc Networks", IEEE ACM Transactions on Networking,volume 16,No.4,PP.791-802,2009.
[10] Thongchi Chuachan and Somnuk Puangpronpitag ,"A Noveel Challebge & Response Scheme Agaist Selective Forwarding Attacks in MANET", IEEE, 2013.
[11] Hung-Min Sun ,Chiung-Hsun Chen and Yu-Fang Ku ,"A novel acknowledgment-based approach against collude attacks in MANET", Elsevier,pp.7968-7975,2012
[12] DjamelDjenouri and NadjibBadache,"On eliminating packet droppers in MANET: A modular solution",Elsevier,pp.1243-1258,2009.
[13] M.Shila, Y.Cheng and T.Anjali," Mitigating Selective Forwarding Attacks with a channel aware approach in WMN", IEEE Transaction on Wireless Communication, Vol.9, No.5, PP. 1661-1675,2010.
[14] KashyapBalakrishnan, Jing Deng and Pramodk.Varshney, " TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks" , IEEE Communication Society,PP. 2137-2142,2005.
[15] S.FESLINANISH MON, RAJ KUMAR SHAH, L.RAJAJI, " A PROGRESSION BASED METHOD FOR THE DETECTION OF BLACK AND GRAY HOLE ATTACKS IN MANET", IJCNWMC, Volume 3,Issue 3,PP. 33-40,August,2013.
[16] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," IETF, RFC 2501, January 1999.
[17] G.Dini and A. Duca, "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network," Ad Hoc Networks, vol. 10,2012, pp. 1167-1178
[18] R. Akbania, T. Korkmazb, and G. V. Rajuc, "EMLTrust: An enhanced Machine Learning based Reputation System for MANETs," Ad Hoc Networks, vol. 10,pp. 435-457,2012.
[19] K. Balakrishnan, J. Deng, and P. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," in the Proceeding of IEEE Wireless Communications and Networking, New Orleans, LA, USA,pp. 2137-2142,2005.
[20] H.-M. Sun, C.-H. Chen, and Y.-F. Ku, "A novel acknowledgmentbased approach against collude attacks in MANET," Expert Systems with Applications, vol. 39, July 2012.
[21] W. Li, J. Parker, and A. Joshi, "Security Through Collaboration and Trust in MANETs," Mobile Networks and Applications, vol. 17, pp. 342-352, 2012.
[22] A. Mitrokotsa and C. Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection," Ad Hoc Networks, 2012.
[23] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34,pp. 107-117,2011.
[24] Z. Ziming, H. Hongxin, A. Gail-Joon, and W. Ruoyu, "Risk-Aware Mitigation for MANET Routing Attacks," IEEE Transactions on Dependable and Secure Computing, vol. 9,pp. 250-260,2012.
[25] T. Shu and M. Krunz, "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing," in the Proceedings of the ACM conference on Security and Privacy in Wireless and Mobile Networks, Tucson, Arizona, USA,pp. 87-98,2012
[26] J. Chen, R. Boreli, and V. Sivaraman, "Improving the efficiency of anonymous routing for MANETs," Computer Communications, vol. 35 May 2012.
[27] H. Xia, Z. Jia, X. Li, L. Ju, and E. Sha, "Trust prediction and trustbased source routing in mobile ad hoc networks," Ad Hoc Networks, 2012.