ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Review of Isolate and Prevent Selective Packet Drop Attack in MANET

SagarPatolia[1], HarmandeepSingh[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 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. There was notorious security problem in MANET. In this paper we will discuss about various routing protocol e.g. AODV (Ad-Hoc On-Demand Distance Vector), DSR (Dynamic Source Routing)]. Isolate possible attack on ad-hoc network and prevent it with numerous techniques.

KEYWORDS:MANET, AODV, DSR, ATTACK-Selective packet drop

I. INTRODUCTION

Mobile Ad Hoc Network is a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized or centralized administration[2]. MANET works with dynamic topology and make temporary network for communication. This type of network works on multi hop reachability for replay packet to destination throughout in network.

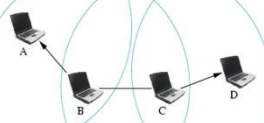

Fig. 1. Mobile Ad-Hoc Networks

Due to its characteristics like dynamic topology resource constraints ,infrastructureless environment and limited physical security its is vulnerable to no of attacks[7].Security is an essential service for wired and wireless network communication. The Success of MANET strongly depend on whether it is secure from outside network. However, the charateristics of the MANET pose the challaenges and oppertunities in acheving the security goals. There are variety of attacks that target the weakness of MANET. For eg. Attacks on routing message which are an essential component of mobile network communications. There are many possibility that the intermediate node being melicious node and attacks to target the route dsicovery or maintenance phase and disrupt the communication. There are also some attacks that trigger on particular routing protocols such as DSR or AODV. The aim of the study is to detect and isolate the selctive packet drop attack using AODV protocol. The malicious node is responsible for dropping packet node after advertising itself as the valid path to source node. The selcctive packet drop attack is difficult to detect and prevent.

DOI: 10.15680/IJIRSET.2014.0312042

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

This attack degrades the network performance and leds to denial of service of attack. The attack is triggerd by the malicious node which is present in the network.

II. CHARACTERISTICS OF MANET

- Dynamic Topology: MANET is made up of mobile nodes, for this any node can be frequent change so any random or dynamic topology required to establish communication.
- Multihop Routing: In Ad-Hoc multi-hop routing is very important factor,, Becsause one node want to broadcast its packet information to destiantion nodebeyond its scope outside networkrange.packet should pass with number of intermediate or neighbour node.
- Limited Bandwidth : Bandwidth is law compare to wired network is law due to stale routes ,various noise, distortion and fadding effect.
- Autionomous(Region or Orgiation) Node[Terminal]: In mANET each node is act as host and router depend on the situation of communncation so it is called Autonomous system(AS).
- Energy Constrained Operation: Some or all MANET nodes relay on batteries so important challenges is to design the system to consume law battery power.
- Limited Physical Security: Mobile nodes or AS(autonomus system) node is vulnerable or malicious from attacker than wireeed network.So such, Attacks are possible which increase security threats like evasdroping, spoffing, Denial of service attack.[2].

III. AD-HOC ROUTING PROTOCOL

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 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.

DOI: 10.15680/IJIRSET.2014.0312042

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

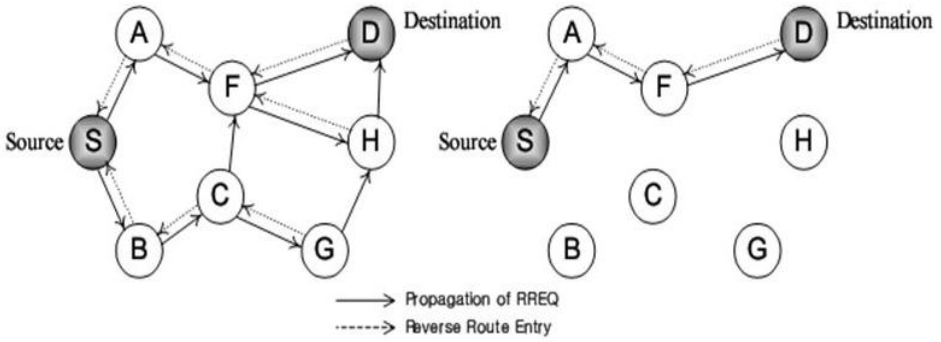

Fig.2. (a) RREQ Braodcast (b) RREP Forwardpath (Route Determination From Source to Destination)

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. SECURITY THREATS IN WIRELESS AD-HOC NETWORKS

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) Black-hole attack[12]: 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.

D) 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.

E) Selective Packet Drop Attack: Packet drop attack is some what releated to black-hole attack but it hard to detect and prevent it. In this attack node is suppose to replay to peer one, it discard them to deny of message or disrupt the network[10,11].The melicious node can accomplish this attack selectively so it is callled selected 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 overcome this problem Thongchai and Somnuk et al.discuss the previous

DOI: 10.15680/IJIRSET.2014.0312042

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

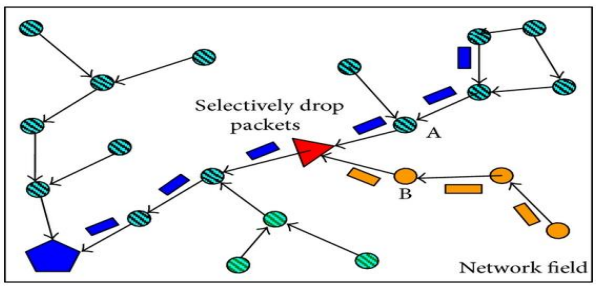

Fig.3.Selective Packet Drop Attack

Proposed technique which is based on acknowledgement based and reputation based. They observe that the problem arise because of misbehaving and selfishness of the intermediate node and the result was packet drop at mid of the path. 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 use the key distribution technique (KD) to secure routing and it will provide the confidentiality that the legitimate source send these packet.

V. LITERATURE REVIEW

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).

Bo Sun, Yong Guan et al. [12],In this paper they proposed a neighbour 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 datashows when we simulate 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.

Tien-Ho Chen and Wei-Kuan Shih et al. [13] In this paper they discussed about importance of mutual authentication for wireless sensor networks .They also discussed about the DES protocol which is the hash-based authentication protocol. This protocol provides the security aligned with the stolen verifier, replay, masqueradeand guessing attacks.

Pradeepkyasanur etal. [14] proposed a protocol extension of 802.11 DCF protocol to detect the selfish behaviour of the nodes in the infrastructure and ad hoc network topologies. The Selfish nodes means nodes which select the contentional window (CW) time in such a way so that the other nodes are keep on waiting to send the data and overall through put of the network degrade [11]. The proposed scheme has three components first one is that the receiver decides that whether sender is diverting form protocol or not. Second component is penalize ,in this scheme the receiver assigns the contentional window time to the sender if sender not sends data in that time period sender have to pay the plenty. Plenty means that in next time when sender sends that data they have to wait more to send data to receiver .The third component is the diagnosis scheme receiver decide 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 form that sender.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Ahmed M.Abd EL-Haleem and IhabA.Ali etal. [**17],** Propose mythology to isolate packet dropping attack by using two disjoint routesprotocol 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 behaviour 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 etal.[18], Propose technique to secure transmission in the MANET using Ad-Hoc On-Demand routingprotocol(AODV). Due to lack of resource and infrastructure ad-hoc network is not able to prove logical operation. Proposed schema called Enhanced Adaptive Acknowledgement (EAACK) which raise 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(Misbehaviour report authentication).

VI. FUTURE WORK ANDCONCLUSION

Mobile ad-hoc network have been wast area of research work from past few years because its widely used application in battlefield and business purpose. Due to openness and dynamic topology network is vulnerable from attacker. In this paper we have discuss MANET protocol, its characteristics and attack which trigger on it. We have discuss various technique to isolate and prevent selective packet drop attack which degrade the system performance by decreasing latency, throughput and increasing end-to-end delay. There are acknowledgmentsand IDS based schema which prevent this attack in AODV protocol. In our feature work we proposed new algorithm based on monitor node technique to which improves network efficiency.

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.
[10] Thongchi Chuachan and Somnuk Puangpronpitag ,"A Noveel Challebge & Response Scheme Agaist Selective Forwarding Attacks in MANET", IEEE, 2013.
[11] 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. 1661-1675,210
[12] Bo Sun, Yong Guan, Jian Chen, U.W.Pooch,"Detecting black-hole attack in mobile ad hoc networks",Personal Mobile Communications Conference,5th European (Conf. Publ. No. 492),2003.
[13] Tien-Ho Chen and Wei-Kuan, Shih , "A Robust Mutual Authentication Protocol for Wireless Sensor Networks"*ETRI Journal*, Volume 32, Number 5, October 2010.
[14] Pradeepkyasanur "Selfish MAC layer Misbehavior in wireless networks", IEEE Transaction on Mobile Computing,Volume-4, Issue 5,pp. 502-216,2005.
[15] KashyapBalakrishnan, Jing Deng and Pramodk.Varshney, " TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks" , IEEE Communication Society, PP. 2137-2142,2005.
[16] 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.
[17] 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.
[18] K.Sangeetha ," SECURE DATA TRANSMISSION IN MANETS USING AODV", IJCCER, Volume-2,Issue 1,PP. 17-22, 1 January 2014.