IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Survey of Black Hole Detection Technique in MANETs

Pooja

M.Tech Scholar, Department of Computer Science & Engineering, BPS Mahila Vishvavidyalya, Khanpur Kalan, Sonipat, Haryana, India

Abstract: Mobile ad hoc network (MANETs) is emerging research field of wireless network. MANETs is temporary network in which collection of node are connected in dynamic topology without any existing central administrator. Because of self infrastructure, different types of security threats are also increasing day by day. Black hole attack is one of the security threats against MANETs routing. Black hole is malicious node in which this malicious node claim itself that shortest path from source and destination but in actual it will all packet destroyed or dropped all packet after received from source. In this paper, we discussed black hole mitigation techniques which proposed by researchers. We have also studies about pros and cons of detection techniques as based on proactive and reactive routing in MANETs.

Keywords: mobile ad hoc networks, routing protocols, black hole attack, collaborative black hole attack, AODV, DSR.

1. INTRODUCTION

Mobile Ad Hoc Networks are self-sufficient and without a centralized administration wireless systems. MANETs are collection of mobile nodes that are free moving in and out in network environment. Node as a mobile phone, MP3 player, laptop etc. these nodes are taking action as host/router according to network requirement. The node are self-configuration because are that are need any infrastructure. For example mobile phone connected to Wi-Fi without any specific cable but connectivity in specific arbitrary topologies through wireless link.
MANET working group developed IP routing protocols because of self-infrastructure. Routing protocols is one of the tricky and remarkable research fields for researchers. MANETs are many applications like Military networks, emergency service, sensor network, automotive applications etc. So according to above specification of MANETs security issue are more are more are challenging for communication and transmission since there security threat are increasing day by day. Security threat as Black Hole, Worm Hole, Denial of service (Dos), Sybil attack, flooding attack, routing table overflow attack, selfish node misbehaving, impersonation attack etc.

In this paper we are discussing about Black Hole attack in MANETs. In 1st section we describe introduction (already described), 2nd section characteristics of MANETs, 3rd section we will describe routing protocol and in 4th section describe black hole attack 5th proposed solution for MANETs.

1. MANET CHARACTERISTICS

1. Dynamic network topology-
An Ad hoc Network are change route frequently because in MANETs have self structured network so sometime packet loss and also leading network partitions.

2. Autonomous and infrastructure less-
MANET has self-infrastructure and centralized network administration. Each node works as a router/host and operates in circulated manner.

3. Multi-hop routing-
Since there exists no committed router, so every node also acts as a router and aids in forwarding packets to the anticipated destination. Hence, information sharing between mobile are available.

4. Variation on link and node capabilities
Difference types of radio device that have transmission capabilities have equipped with participating node in an ad hoc networks. These Radio devices operate on multiple frequency bands. Because of radio capabilities asymmetric links are formed in MANETs network.

5. Energy-constrained operation-
Every portable device is carried limited power supply battery so power is restricted.

6. K scalability-
A wide range of MANETs applications may involve massive networks with plenty of nodes especially that can be found in premeditated networks. Scalability is critical to the blooming operation of MANET. [1]

2. ROUTING PROTOCOLS

There basically three type of routing protocol in MANETs:

3.1 Table driven or Proactive routing protocol
In this routing every node of routing maintains information in table and the router discovery process

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

based on periodically update. The main disadvantages of such algorithms are:

1. Particular amount of data for maintenance.
2. Time-consuming response on reorganization and failures.

Proactive are proposed many routing protocol like DSDV, WRP, GSR, HSR, FSR, OLSR, CGSR, STAR, MMWN etc.

3.2 On-demand or Reactive routing protocol

On demand or reactive routing protocols were intended to minimize overhead in proactive routing protocols. The route of next or destination node are discovered and maintained when these are required mean we not store all information in advance as table driven routing. Reactive routing discovered node by broadcasting hello message. Destination can used link reversal or piggybacking for reply message to sender in route. The on demand routing is based on source routing and hop to hop routing. In source routing data packet carried all information from source to destination. In hop to hop routing data packet stored destination address and next node address. The main disadvantages of such algorithms are:

1. High latency time in route discovery.
2. Unnecessary flooding can lead to network congestion.

Reactive routing protocol proposed AODV, DSR, LMR, TORA etc.

3.3 Hybrid Routing Protocols

Hybrid routing protocol are combine both reactive and proactive routing protocol properties. In this network are divided into zone or some tree structure or clustering. In this protocol initially established proactive routing and additionally active node as flooding mean use reactive protocol. Other method requires predetermination for typical cases. The main disadvantages of such algorithms are:

1. Improvement depends on number of other nodes activated.
2. Response to traffic demand depends on grade of traffic volume.

The Hybrid routing protocol proposed Zone Routing Protocol (ZRP), Zone one-based Hierarchical Link State (ZHLS). [2]

3. BLACK HOLE ATTACK

In black hole attack, malicious node use routing protocol as claims itself shortest path to destination so according to malicious node specification, sender or neighbor node of malicious node will route packet to malicious node for forward to destination but it will be dropped the packet or discard the packet. Black hole means malicious node advertising itself by routing protocol.

In this way attacker node will always have accessibility in replay to the route request and thus stop the data packet and hold on it. So when malicious node route established, now it's totally dependent at malicious device that it will hold or drop the packet or send to next address.

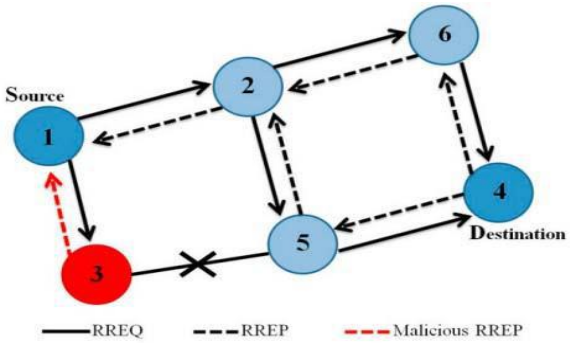

Fig. 1 Black Hole Attacks [4]

In given figure sender "1" wants to send packet to destination "4" so begin route discovery process. Now node"1" is route request packet (RREQ) message flooding. When malicious node "3" receive broadcast message so it will send route reply packet (RREP) to a node before any other node response. Node "1" will think that C have activate route so it will send the entire data packet to "3" node and ignore other node RREP requests. So now all packets are dropped and retain it [3] [4].

4. LITERATURE REVIEW

1. Sun B, Guan Y, Chen J, Pooch UW [5] are proposed solution for black hole attack by using AODV, it also used in DSR routing with minor modification in given method. The neighborhood based method is engaged to recognize the unverified nodes, and the sender sends Modify_routing_packet to renew routing path to destination in recovery protocol. In this proposal routing overhead does not increase and also give probability of accurate detection solution is also achieved. But this proposal is useless when attacker send multiple fake reply messages so this solution is best for single black hole attack in routing.

2. Al-Shurman M, Yoo S-M, and Park S [6] proposed solution in two way for AODV routing. In first solution, examine the number of route from source to destination mean find the redundant route in between source to destination node and source node find out safe route. Second solution provides the unique sequence number accumulated and its value higher than current sequence number. According to simulation result it's minimize the network overhead because it have used to inbound cryptography. But both methods are applicable for single black hole attack in MANETs. Both solutions easily cracked by attackers in collaborative black hole node.

3. William Kozma Jr. et al. [7] are proposed REAct scheme that are detection approach for reactive misbehavior node. REAct scheme automatically triggered when performances are degraded form source to destination. REAct based on three phases: (a) the audit phase, (b) the search phase and (c) the identification phase .this scheme also applicable for

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

single black hole attack in DSR routing. It will decrease communication overhead but incremented in identification delay.

4. Raj PN, Swadas PB [8] were proposed Detection, Prevention and Reactive AODV (DPRAODV) Scheme which will use new control packet that's called ALARM. ALARM is blocked malicious node but it's not processed. According to scheme, black hole attack will be detected but also prevented by updating threshold the realistic network environment. DPRAODV have high packet ratio then normal AODV but it will increase high network overload and end to end delay.

5. Ming-Yang Su [9] proposed Anti-black Hole Mechanism (ABM) based intrusion detection system (IDS). ABM of employment two additional tables called RQ table and SN table, RQ table for RREQ packet and SN table for RREP packet. In starting of use as ABM function in sniff mode when IDS executed node. ABM will use for estimated the value of suspicious node. If the value cross limit from predefined threshold value, it can be belong as a black hole. In this, the packet loss rate can be decreased to 11.28% and 14.76% but it is not applicable for collaborative black hole attack.

6. Sanjay Ramaswamy et al. [10] proposed detection solution for collaborative black hole by using data routing information (DRI) table and cross checking method also develop modified AODV routing protocol. In this method every node have developed extra DRI table, in which "0" for false and "1" for true. The entry is collected of two bits, "From" and "Through". These methods are proposed only theoretically not simulated result.

7. Weerasinghe et al. [11] proposed that DRI table and cross checking using FREQ and FREP for modification of cooperative black hole attack. According to paper the simulation result for modified AODV have higher throughput performance almost 50% than AODV and 5-8% more communication overhead of route request.

8. Chang Wu Yu et al. [12] proposed DCM (distributed and cooperative mechanism) for detection of collaborative black hole attack. In the local data collection phase, each and every node in network have estimation table maintained. Global reaction phase use for warning message for whole network. As a simulation result, The Packet data ratio is enhanced from 64.14 to 92.93%, and the detection rate is higher than 98% but communication overload is higher than AODV.

9. Min Z and Jiliu Z [13] proposed Hashed-based MAC (message authentication code) and Hash-based PRF (pseudo random function) Scheme. These both proposals suitable for detection of collaborative black hole attacks by using fast message confirmation and group recognition, provide secure routing by find out suspicious node from communication. According to paper, the simulation result proof that data packet delivery ratio higher than simple AODV but communication overload and transmission delay higher than ordinary AODV. Disadvantage of this proposal is malicious node is able to send unlimited fake reply to dart the detection scheme.

10. K.Selvavinayaki et al. [14] proposed solution by using public key infrastructure to provide security to DSR routing path.

11. Gurbir Singh et al. [15] provide solution for remove selective black hole attack in Dynamic source routing (DSR) by using ALARM system. According to paper the packet delivery ratio is faster than ordinary DSR.

12. Sanjeev Sharma et al. [16] proposed solution for black hole in ZSR by using bluff probe method. According to simulation result the network overload is minimum but it method applicable for light weight network**.**

13. Chaitas shah et al. [17] proposed detection method for black hole attack using hybrid technique in which proactive and reactive routing method are combine which also known as zone based routing (zsr).

14. Yasser eirefaie et al. [18] proposed enhance of security for detect black hole attack from zsr routing path. According to paper, it provides higher packet delivery ratio then ordinary zsr. But end to end cost of improvement higher and routing overload increase

5. CONCLUSION

MANETs are self infrastructure and without any centralized administration in wireless network. According to specification of MANETs security issue is emerging research area for researcher. In this paper, we survey of black hole attack and mitigation technique in MANETs and also specified the advantage and disadvantage of techniques according to specified routing. According to survey, proactive routing methods have higher packet delivery ratio but also incremented network overload in due to sporadically broadcasting packet. In reactive routing protocol eliminates network overload in even driven way, but decreasing packet delivery ratio in routing procedure. Therefore in next we studies about misbehavior node detection at based on enhance acknowledgement with cryptography method.

REFERENCES

[1] Jaspal Kumar, M. Kulkarni, Daya Gupta (2013) "Effect Of Black Hole Attack On Manet Routing Protocols",I. J. Computer Network and Information Security, Published Online April 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis. 2013.05.08

[2] Devendra Singh, Anuj Singh, S.S. Bedi (2015) "Intrusion Detection System For Blackhole In Manets", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 12, December 2015, ISSN: 2277 128X.

[3] Mohamed Elboukhari, Mostafa Azizi and Abdelmalek Azizi(2015) "Impact Analysis Of Black Hole Attacks On Mobile Ad Hoc Networks Performance", International Journal of Grid Computing & Applications (IJGCA) Vol.6, No.1/2, June 2015, DOI:10.5121/ijgca.2015.6201

[4] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Tseng et al. Human-centric Computing and Information Sciences 2011, 1:4http://www.hcis-journal.com/content/1/1/4

[5] Sun B, Guan Y, Chen J, Pooch UW "Detecting Black-Hole Attack In Mobile Ad Hoc Networks". Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003

[6] Al-Shurman M, Yoo S-M, Park S "Black Hole Attack in Mobile Ad Hoc Networks". Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004

[7] William Kozma, Lazos L "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits". Paper presented at the Second ACM Conference on Wireless Network Security, Zurich,Switzerland, 16-18 March 2009

[8] Raj PN, Swadas PB "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET".International Journal of Computer Science 2:54–59. doi: abs/0909.2371

[9] Ming-Yang Su Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications 34(1):107–117. doi:10.1016/j.comcom.2010.08.007

[10] Sanjay Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K (2003) "Prevention of Cooperative Black Hole Attack inWireless Ad Hoc Networks" Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada,USA, 23-26 June 2003.

[11] Weerasinghe H, Fu H "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation". Paper presented at the Future Generation Communication and Networking, Jeju-Island,Korea, 6-8 December 2007

[12] Yu CW, Wu T-K, Cheng RH, Chang SC "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network". Paper presented at the PAKDD workshops, Nanjing, China, 22-25 May 2007

[13] Min Z, Jiliu Z "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks". Paper presented at the International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 16-17 May 2009.

[14] K.Selvavinayaki K.K.Shyam Shankar Dr.E.Karthikeyan (2010)"Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs". Paper presented at International Journal of Computer Applications (0975 – 8887) Volume 7– No.11, October 2010

[15] Gurbir Singh, Nitin Bhagat (2015) "Removal of selective Black hole attack in Dynamic Source Routing (DSR) Protocol by alarm system" International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-6, June 2015

[16] Sanjeev sharma, Rajshree, Ravi Prakash Pandey, Vivek Shukla, (2009) "Bluff-Probe Based Black Hole Node Detection and prevention". IEEE International Advance Computing Conference (IACC 2009), March 2009

[17] Chaitas Shah, Manoj Patel (2014) "Improving ZRP Protocol against Blackhole Attack." International Journal of Engineering Development and Research (www.ijedr.org) 1939, 2014 IJEDR | Volume ,Issue 2 | ISSN: 2321-9939

[18] Yasser EIRefaie, Laila Nassef, Imane Aly Saroit (2013) Track "Enhancing Security of Zone-Based Routing Protocol using Trust".The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May 2013 Computer Networks