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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Literature Survey of MANET under Blackhole and Grayhole attack

Tejasvi Thanvi[1], Neeraj Arora[2], Piyush Vyas[3]

Student of B.Tech, Department of Electronics & Communication Engineering, JIET, Jodhpur, India[1]

Convener (Assistant Professor), Computer Science Department, Vardhman Mahaveer Open University, Kota, India[2]

Assistant Professor, Department of Electronics & Communication Engineering, JIET, Jodhpur, India[3]

Abstract: A mobile ad hoc network (MANETs) is infrastructure-less network where nodes communicate with each other without any centralized administration. MANETs are prone to various kinds of security attacks due to its nature as mobile and open media. Blackhole and Grayhole are one of them. The impact of both attacks is most drastic. In both attacks, attacker attracts traffic by claiming that it has shortest route to the required destination and then simply drops the packets. As a result, efficient techniques to detect and prevent blackhole and grayhole attack are needed. In this paper, a review on different existing techniques for detection and prevention of blackhole and grayhole attack are presented.

Keywords: MANET; OLSR; AODV; ZRP; Black hole attack; Grey hole attack.

I. INTRODUCTION

The latest advancement in wireless technology and its applications received a lot of attention. An ad hoc network is one such recent technology, which gives a new paradigm for wireless self-organized networks. Mobile Ad-Hoc Networks (MANETs) are autonomous, self-organized, with no fixed infrastructure and decentralized wireless systems. Each node in the MANET has to take care of the routing aspects as well. There are many routing protocols available for routing in ad-hoc networks. The routing protocols for MANETs are broadly classified into two types as proactive and reactive. The protocols like DSDV, OLSR, OSPF, are proactive protocols which will use periodic messages in order to know the network topology. The reactive protocols include AODV, DSR.

Because of decentralized nature and having dynamically changing topologies, MANETs are vulnerable to various kinds of threads and many of them target the routing protocols. The mobility of nodes makes it more vulnerable. There are two types are attacks: passive and active attack. A passive attack does not disrupt the operation of the protocol, but attempts to figure out valuable information by listening to traffic. Instead an active attack disrupts the operation of the protocol in order to gain unauthorized access, circumscribe availability or degrade the network performance. Some of them are, wormhole attack, blackhole attack, grayhole attack, byzantine attack, rushing attack etc.

II. BLACKHOLE ATTACK

Blackhole attack is a kind of active attack. In this attack, Blackhole immediately sends a false route reply messages when it receives an RREQ message, without checking its routing table. These false route reply messages are to inform other nodes in the network that the destination is on the next hop from this attacker node and the attacker node has the best route to that destination. All neighboring nodes update their routing tables and make the attacker node their next hop for the destination. Now when this attacker node receives the data packets, it drops all the packets and the packets do not reach the destination.

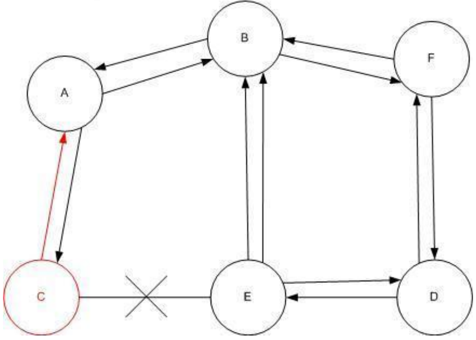

Fig 1. Node C is a Black hole.

III. GRAYHOLE ATTACK

Grayhole attack is an extension of Blackhole attack in which a malicious node's behavior is exceptionally unpredictable. The grayhole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the blackhole attack where the malicious node drops the received data packets with certainty. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of grayhole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also

DOI 10.17148/IJARCCE.2015.4982

exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.

IV. Techniques for Prevention and Detection of Blackhole and Greyhole Attacks

In [4], Jaydip Sen et al. use AODV as their routing protocol and simulation is done in ns2 simulator. They first mention some practical assumptions that have been made for formulating the network model. The proposed mechanism involves both local and cooperative detection to identify any malicious gray hole node in the network. The mechanism consists of four security procedures which are invoked sequentially. The security procedures are: (1) Neighborhood data collection, (2) Local anomaly detection, (3) Cooperative anomaly detection, and (4) Global alarm raiser. In local data collection, each node collects information through overhearing packets to evaluate if there is any suspicious node in its neighborhood. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious gray hole node. Subsequently, the cooperative detection procedure is initiated by the initial detection node, which proceeds by first broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one. As soon as a confirmed gray hole node is identified, the global reaction is activated immediately to establish a proper notification system to send warnings to the whole network.

In [5], GaoXia openg, proposed a scheme which uses aggregate signature algorithm to trace packet dropping nodes and comprises three related algorithms. 1) The creating proof algorithm. Each node involved in a session should create a proof based on aggregate signature algorithm to demonstrate it has received a message. 2) The checkup algorithm. When the source node suspects that the packet dropping attack has happened, for example, the destination reports that fewer packets have been received than that should be received under normal condition, it will invoke this algorithm to detect the malicious node. 3) The diagnosis algorithm. According to the evidences returned by the checkup algorithm, the source node could trace the malicious node. Simulation is done in ns2 simulator. Simulation results show that our proposal could detect most of the malicious nodes, the false positive rate and the routing packet overhead are low, and the packet delivery rate has been improved. The strengths of proposal are: 1) the reliability is satisfying, as evidence on forwarded packets is used; 2) the application scope is broad, as bi-directional communication links are not necessary; 3) the security is satisfying, as it is hard for malicious nodes to escape detection; 4) the bandwidth overhead is low, as nodes do not need to monitor each other.

In [6], Megha Arya et al. use AODV as their routing protocol. To explain the Gray Hole Attack they added a malicious node that exhibits gray hole, therefore, changed aodv to “grayholeaodv” and proposed protocol is idsaodv (Intrusion Detection System AODV) that is modification of graholeaodv. Simulation is done in NS2 simulator. On the basis of simulation this paper has concluded that Throughput, Routing Load and Packet Delivery ratio is very good recovered through IDS in case of Gray Hole Attack.

In [7], A. M. Kanthe et al. proposed an algorithm to detect gray hole node and eliminate the normal nodes with higher sequence number to enter in black list. The algorithm calculates and checks the peak value whether reply packet sequence number is less than or not. The parameters used to calculate the peak value are: a) Routing table sequence number. b) Reply packet sequence number. c) Elapsed time of ad hoc network which is analogous to current simulation time of simulator in simulation environment. d) Total number of reply packets received by theintermediate/neighbour/replying node. e) Reply Forward Ratio (RFR) of replying node.

In [8], D. G. Kariya et al proposed an algorithm which is based on a course based scheme. In this scheme, a node observes only the next hop in current route path but does observe every node in the neighbour. In this scheme FwdPacketBuffer is maintained by every node, it is also known as a packet digest buffer. The algorithm is divided into three steps: A) when a packet is forwarded out, its digest is stored into the FwdPacketBuffer and the detecting node overhears. B) Once the action that the next hop forwards the packet is overheard, the digest will be freed from the FwdPacketBuffer. C) The detecting node should calculate the overhear rate of its next hop node and compare it with a threshold in a fixed period of time. The overhear rate of the Nth period of time is defined as OR (N), the percentage of the data packets which are actually received by the destination.

In [9], Mr.ChetanS. Dhamande et al. proposed a technique that focus on the minimizing the impact of gray hole attack using AODV routing protocol. The procedure starts from the starting process, first set the waiting time for the source node to receive the RREQ coming from other nodes and then add the current time with the waiting time. Then in storing process, store all the RREQ Destination Sequence Number (DSN) and its Node ID n RR-Table until the computed time exceeds. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. This is how malicious node is recognized and eradicate. Final process is selecting the next node id that has the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to malicious node recognition in order to continue the default operations of AODV protocol.

In [10], Hizbullah Khattak et al. proposed a solution for avoidance of black / gray hole attacks by discarding the

DOI 10.17148/IJARCCE.2015.4982

first and selecting the second shortest path for data packets transmission. In this way, it becomes difficult for the malicious node to send the RREP message secondly. To be part of the route of the second shortest route, malicious node will have to monitor the entire network which obviously is not an easy task in MANET. They further proposed the hash function for data integrity and detection of these two attacks to ensure more safety and security. Most of the techniques avoid the single blackhole or grayhole attacks but this technique can also prevent the cooperative blackhole and grayhole attacks as well. The proposed solution makes AODV more secure and reliable for data packets transmission.

In [11], Latha Tamilselvan and Dr. V Sankaranarayanan proposed a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid black holes. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. According to this proposed solution the requesting node without sending the DATA packets to the reply node at once, it has to wait till other replies with next hop details from the other neighboring nodes. After receiving the first request it sets timer in the 'TimerExpiredTable', for collecting the further requests from different nodes. It will store the 'sequence number', and the time at which the packet arrives, in a 'Collect Route Reply Table' (CRRT). The time for which every node will wait is proportional to its distance from the source. It calculates the 'timeout' value based on arriving time of the first route request. After the timeout value, it first checks in CRRT whether there is any repeated next hop node. If any repeated next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited. Then it chooses any one of the paths with the repeated node to transmit the DATA packets. If there is no repetition select random route from CRRT. Here again the chance of malicious route selected is reduced.

V. CONCLUSION

Security of MANETs is the biggest challenge because of its nature as infrastructure-less and decentralized. Blackhole and Grayhole is kind of DOS attack which cause the damage to an entire network. These attacks are one of the serious security problems in MANETs. In this paper, we have tried to survey different techniques for detection and prevention of blackhole and grayhole attack in MANET. By this paper we need to find out the work on UDP regarding Blackhole and Grayhole effect with various algorithms. AODV, ZRP, DSDV, OSLR and DSR all routing protocols have 'n' number of users they are unable to understand the behavior of packets flow in the channel. If it drops somewhere, there is no information regarding that drop and then after acknowledgement received in UDP technique.

ACKNOWLEDGMENT

I would like to thankful to all authors who wrote research papers regarding this topic and shared their precious knowledge to create an environment and guidelines to think uniquely in that subject. I would like to thanks my partners also for their given time and work.

REFERENCES

[1] S. Basagni, M.Conti, S. Giordano and I. Stojmenovic, "Mobile Ad Hoc Networking", A John Wiley & Sons, Inc., Publication, 2004, ISBN 0-471-37313-3.

[2] Amara korbaAbdelaziz, Mehdi Nafaa and GhanemiSalim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", IEEE 2013 UKSim 15th International Conference on Computer Modelling and Simulation.

[3] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "DoS Attacks in Mobile Ad-hoc Networks: A Survey", IEEE 2012 Second International Conference on Advanced Computing & Communication Technologies.

[4] JaydipSen, M. Girish Chandra, Harihara S.G., Harish Reddy and P. Balamuralidhar. "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", 1-4244-0983-7/07, 2007 IEEE.

[5] G. Xiaopeng and C. Wei "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks" IFIP International Conference on Network and Parallel Computing, 2007.

[6] JaydipSen, M. Girish Chandra, Harihara S.G., Harish Reddy and P. Balamuralidhar. "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", 1-4244-0983-7/07, 2007 IEEE.

[7] A. M. Kanthe, D. Simunic, R. Prasad "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks" International Journal of Computer Applications , Volume 53, Sep. 2012.

[8] D. G. Kariya, A.. B. Kathole, S. R. Heda "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method" IJTAE, Jan-2012.

[9] Mr.ChetanS.Dhamande and H.R.Deshmukh, "A Efficient Way To Minimize the Impact of Gray Hole Attack in AdhocNetwork ", International Journal of Emerging Technology and Advanced Engineering, Volume 2, February 2012.

[10] HizbullahKhattak, Nizamuddin, FahadKhurshid and Noor ul Amin, "Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash", 78-1-4673-5200-0/13, 2013 IEEE.

[11] LathaTamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), IEEE.

[12] NeerajArora and Dr. N.C. Barwar, "Evaluation of AODV, OLSR and ZRP Routing Protocols under Black hole attack", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 4, April 2014.

[13] NeerajArora and Dr. N.C. Barwar, "Performance Analysis of Black Hole Attack on different MANET Routing Protocols", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014.

[14] NeerajArora and Dr. N.C. Barwar, "Performance Analysis of DSDV, AODV and ZRP under Blackhole attack", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April – 2014.

[15] NeerajArora and Dr. N.C. Barwar, "Performance analysis of DSR, AODV and ZRP under black hole attack", International Journal of Applied Research in Engineering and Science, 2014.

[16] A. Dareshoorzadeh, N. Taheri Javan, M. Dehghan, and M. Khalili, (2008), "LBAODV: A New Load Balancing Multipath Routing Algorithm for Mobile Ad hoc Networks," 6th IEEE NCTTMPC, Malaysia, pp: 344-349.

[17] N. Taheri Javan, A. DareshoorZade, S. Soltanali, and Y. Ghanbari Birgani, (2009), "IZM-DSR: A New Zone-disjoint Multi-path Routing Algorithm for Mobile Ad hoc Networks," 3rd European Symposium on Computer Modeling and Simulation (EMS), Athens, Greece, pp: 511- 516.

[18] T. Clausen and P. J. (Eds.), \Optimized Link State Routing protocol (OLSR)," RFC 3626, IETF Network Working Group, Oct. 2003.

[19] R. Gupta, J. Musacchio, and J. Walrand, \Su±cient rate constraints for QoS °ows in ad-hoc networks," UCB/ERL Technical Memorandum M04/42, 2004.

[20] A. Schrijver, Combinatorial Optimization: Polyhedra and Efficiency. Springer, 2006.

DOI 10.17148/IJARCCE.2015.4982

[21] D.-Y. Hwang, E.-H. Kwon, and J.-S. Lim, "EASR: an energy aware source routing with disjoint multipath selection for energy-efficient multihop wireless ad hoc networks," Proc. Conf. Networking 2006, LNCS 3976, 2006, pp. 41-50.
[22] Stefan Dulman, Jian Wu and Paul Havinga, "An Energy Efficient Multipath Routing Algorithm for Wireless Sensor Networks,"
[23] Hamid Al-Hamadi and Ing-Ray Chen "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks" ieee transactions on network and service management, vol. 10, no. 2, june 2013.
[24] Jian Li ,Yun Li ,Jian Ren and Jie Wu "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks" Ieee transac tions on mobile computing, vol. 12, no. 6, april 2013.

BIOGRAPHIES

Mr. Tejasvi Thanvi receives his B.Tech. Degree in Electronics & Communication Engineering Branch from Rajasthan Technical University, Kota, Rajasthan, India in 2015

Er. Er. Neeraj Arora is Convener (Assistant Professor) of Computer Science Department at Vardhman Mahaveer Open University, Kota. He completed his M.E. in Computer Science Engineering from M.B.M EngineeringCollege. He received B.Tech in Computer Science Engineering from Jodhpur Institute of Engineering andTechnology in 2011. He has published dorzens in national and international conference and journal.His field of interest is Computer Network, Image Processing, Database Management System etc.

Er. Piyush Vyas Completed his B.Sc. Degree in Electroics Engineering Branch from Jai Narayan Vyas University, Jodhpur, Rajasthan, India in 2004, M.Sc. in Electronics Engineering Branch from Devi Ahilya Vishwa Vidfhyalaya University, Indore, MP., India in 2006, and M.Tech. in Communication Engineering Branch from VIT University, Vellore, Tamilnadu, India in 2009. He is Pursuing his Ph.D. degree from Faculty of Engg., ECE Department, MBM Engg. College, JNVU, Jodhpur.

DOI 10.17148/IJARCCE.2015.4982