Analysis of Various Techniques for Isolation of Blackhole Attack

Rama Sharma
Research Scholar
Singhania University, Rajasthan, India

Dr. Amardeep Gupta
Principal, JC DAV College, Dasyua, India

Abstract

The mobile devices are infrastructure less network that are self configured continuously and connected wirelessly makes a mobile ad hoc network (MANET). The MANETs are more prone to different attacks as each device are free to move in any direction without depending on each other. In MANETs there are different type of active attacks like black hole, wormhole, grey hole and sinkhole attacks. Black hole attack is a kind of attacks where a malicious node advertise itself a shortest path during routing discovery and redirect the data towards malicious node. Malicious node dropped data or its desired destination instead of original destination. In this paper, focuses of various prevention and detection methods to detect and prevent the black hole attack.

Keywords

Black hole attack, survey of black hole attack detection and prevention

Introduction

In MANET there is no need of establishing infrastructure or centralized administrator it contain different number of hosts connected wirelessly that are further deployed as a multihop packet radio [1]. The network Architecture is grouped into main three categories [2]:

a. Enabling Technologies: The Body (BAN), Personal (PAN), local(LAN) , metropolitan (MAN) and wide (WAN) area networks are different classes depending on the coverage area of network [9].

b. Networking: The peer-to peer communication environment self-organizing, dynamic, volatile behaviors of MANET that makes it need to re-design most main functionalities of the networking protocols.

c. Middleware and applications: The rapid development of mobile ad hoc networks has grown the use of MANETs in military applications. The standard community as well as commercial business industry has gained a lot of interest that require a development in Manet's devices.

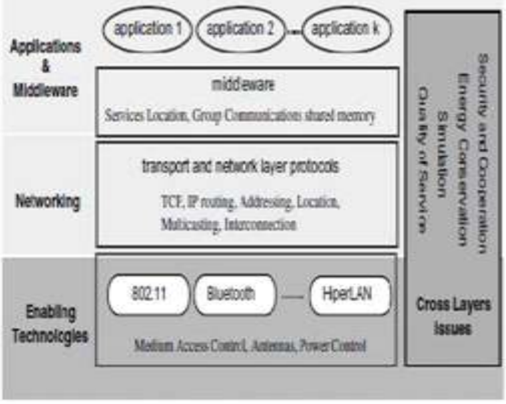
Applications & Middleware
application 1
application 2
application k
middleware
Services Location, Group Communications shared memory
Networking
transport and network layer protocols
TCP, IP routing, Addressing, Location, Multicasting, Interconnection
Enabling Technologies
802.11
Bluetooth
HiperLAN
Medium Access Control, Antennas, Power Control
Security and Cooperation
Energy Conservation
Simulation
Quality of Service
Cross Layers Issues

Fig1. MANET Architecture [2]

In MANET, environment gets affected due to number of issues that creates restrictions and inadequacies [3].

a) Restricted wireless transmission range: In wireless network there is restricted radio group that results in restriction of data that can be provided by the network.

b) Time-varying wireless link characteristics: The path harm, obstruction and declining intervention are different broadcast disorder on which channel of wireless depends. The wireless transmission features such as data rate, consistency are restricted.

c) Broadcast nature of wireless medium: The devices have some restrictions on transmission and broadcast nature of radio channel that affects the transmission coverage area of the network.

d) Packet losses due to transmission errors: In wireless channel the extraordinary bit error rate (BER) damages the package of Ad hoc wireless networks.

MANETs Security: The security services and Attacks are the two important security aspects that have been considered in network. The Availability, Authentication, Data confidently, integrity and non-repudiation are five important security service protecting policies that makes a network secure [4]. While attacks use network vulnerabilities to defeat a security services, some of most important attacks in MANETs are like Black hole attack, Worm hole attack, Byzantine attack, Snooping attack, Routing attack, Session hijacking, denial of service, jamming attack, modification attack, fabrication attack, man-in-middle attack, gray hole attack.

Black hole attack: This attacks comes under the denial of service attack by which all the packets are attracted by malicious node by claiming the shortest path for the destination [5]. Once packets has been captured by malicious node it will drop all packets rather than forwarding it to the destination. The malicious node affect in the group in case of cooperative black hole attack [7] for its example the shown criterion in fig 2 has been considered. In this the destination node is denoted as D and source node as S and all the nodes between 1 to 5 will comes under the category of intermediate nodes. The cooperative black holes are node no. 4 and 5. The RREQ packet requests is sent to neighboring nodes in case of when source node want to transmit data packet to destination. The RREQ is immediately sent to source code even when it is received by malicious node and that data is dropped by black hole node when data is transmit by source node.

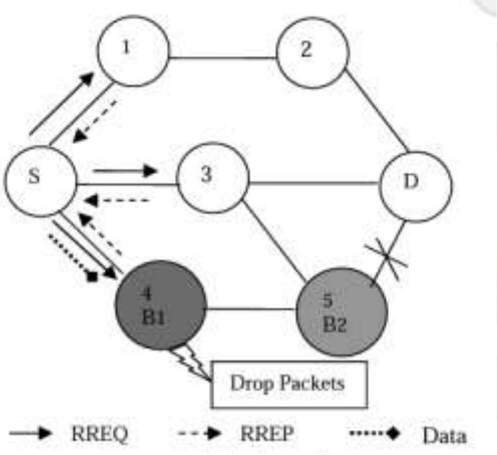

Fig 2. Black hole attack [5]

Literature Review

Jydip sen et.al [1] proposed a mechanism for detection of cooperative black hole attack. In mechanism used two concepts to modify the AODV protocol. First one is DRI (data routing information) table and second is cross checking. Each node maintains a DRI table. In DRI table have information about true or false values. In cross checking when source node (SN) broadcast a RREQ message to discover a secure route, intermediate node (IN) generates RREP to provide information about its DRI table. BY using this mechanism delivery ratio is increased 38% to 55%. This results in an average improvement of 17%, but performance is decreased.

Yanzhi Ren et.al [2] described a technique to detect black hole attack in disruption-tolerant networks through packet exchange recording. In this technique, two tables RRT (receiving record table) and SRT (self-record table) used to keep the record of exchanged packets. RRT have the packet exchanged record of that node which sends the RREP and SRT have packet exchange record of that node which sends the RREQ. By using this technique detect insider attack efficiently with high detection rate and low positive rate.

H.A. Esmailli et.al [3] purposed a scheme to analysis the performance of AODV protocol under black hole attack through use of OPNET simulator. In this paper discuss two approaches to secure MANET. First is the securing ad-hoc routing by using various protocols like DSR (dynamic source routing), DSDV (destination sequence distance vector), ARAN (authenticated routing certificate process), TRP (real time transfer protocol) etc. A method is introduced by the intrusion detection system in which next hop RREP message information is sent back by each intermediate node. In the presence of black hole attacks there is reduction in PDR and increase in the packet delivery ratio.

Mohite Raga et.al [4] described mechanism to detect cooperative black hole attack by using cooperative security agents. In mechanism take three concepts, first is SRT and RRT Tables, second one is data routing information and third is cooperative security agents(they detect and generate alert notifications for other nodes to avoid cooperative black hole attack).by using this mechanism malicious nodes detect effectively and mitigate the negative impact caused by black hole and cooperative black hole attack.

Mohammad Al-Shurman et.al [5] purposed two solutions to detect the black hole attack. First solution is based on RREP packet arrives from more than two nodes. This method is secure but longer time delay. Second solution is based on RREP with record of Last-packet sequence numbers. Second method is fast, reliable and reduces the overhead in network. But this solution is not secure because sometimes attacker node can listen to channel and Update the tables.

Osathanunkul zhang et.al [6] purposed a scheme to detect black hole attack by using S-ETX (secure-expected transmission count). S-ETX is improved version of ETX. Two modifications is done in S-TEX, first is df and dr values calculated by initiator and second is keep record by initiator which packets are received. By using SETX the performance is increased and cost overhead is also reduced.

Raj Swadas et.al [7] described DPRAODV (Detection, prevention and Reactive AODV) for detection and prevention of black hole attack. In DPRAODV, when AODV receive RREP then it checks the sequence number of node. If sequence number is higher than threshold value then surmise a malicious node, and add it in a block list, and ALRAM packet is send to another neighbor nodes. By using DPRAODV packet delivery ratio is increased and normalized routing overhead, but increases the traffic load.

Tamilselvan Sankaranarayanan et.al [8] purposed a mechanism to prevent the black hole attack by using "Fidelity Table" concept. Fidelity table keep the record fidelity level of nodes. If fidelity level is less than threshold value then it declares malicious node. By using this mechanism packet delivery is increased but overhead is increased, due to fidelity table is added.

Songbai Lu et.al [9] described the SAODV (secure AODV) protocol to provide the more security to AODV. Main difference between them is routing discovery process. By using SAODV protocol packet loss is reduced. In AODV packet loss is 57% but in SAODV 8.132%, so 49% packet loss is reduced.

Hongmei Deng et.al [10] purposed a Solution to provide routing security in wireless ad hoc networks. In which, the role of intermediate node ends, all reply message is send only by the destination node. This solution is effectively only detecting the black hole attack but cooperative black hole attack is not controlled.

Kaur and karle et.al [11] purposed a verification technique "digital signature" for detection and prevention of black hole attack. In which at destination TTL scheme is used to select the shortest path from different nodes. At destination node a digital signature column in which have the digital signature of every visiting node. This technique is effectively reduced cooperative black hole attack.

Ayesha Siddiqua et.al [12] purposed a secure knowledge algorithm to prevent the black hole attack in MANETs. In which, every node monitor other all neighboring nodes, and nodes compare information of its neighbor node with its knowledge table. In knowledge table have information about fm & rm values of node. If nodes fm value does match with rm value, that node declare as a malicious node.by using this algorithm, finds packet drop reason before claiming node as a black hole node.

T. Manikandon et.al [13] purposed a scheme to remove the selective black hole attack in MANET by using AODV as reactive protocol. In MANET the selective black hole attack is considered as malicious node attacks that effectively produces a route for destination. The sequence number and hop count of the routing message has been ignored while selecting the route for destination. Purposed scheme based on three concepts Protocol description, Selective black hole discovery process and performance analysis.

S. No	Author	Method Name	Protocol	Tool	Prevention & Detection	Remark
1	Jydip Sen et.al[1]	DRI Table & cross checking	AODV	NS-2	No/Yes	Packet delivery ratio is increased by 17% but performance is decreased.
2	Yanzhi Ren et.al[2]	RRT & SRT Tables	PROPHE T	NS-2	No/Yes	It has low positive rate and high detection rate in terms of effectively detecting insider attack.
3	H.A.Esma il-i et.al[3]	Securing ad-hoc routing & intrusion-n detection	AODV	OPNE-T	No/Yes	Packet delivery is reduced in presence of black hole attack.
4	Mohite Raga et.al[4]	Various cooperative security agents	AODV	NS-2.35	No/Yes	Malicious node detects effectively and reduces negative impact caused by black hole attack.
5	Mohamm andAl-Shruman et.al[5]	RREP Stash Mechanism	AODV	NS-2	Yes/Yes	Detect single black hole attack node.
6	Osathanun kul Zhang et.al[6]	SETEX Protocol	ETX	NS-2	No/Yes	Performance is increased and cost overhead is also reduced.
7	Raj	DPRAODV:Soluti	AODV	NS-	Yes/Yes	Packet delivery ratio is

	Swadas et.al[7]	on against black hole attack		2.33		increased and normalized routing overhead.
8	Tamilselvan Sankaranaryan et.al[8]	Prevention of cooperative black hole attack by using Fidelity Table	AODV	GLOMOSIM	Yes/Yes	Packet delivery ratio increases but delay is also increased.
9	Songbai Lu et.al[9]	Secure routing protocol-SAODV	AODV	NS-2	Yes/Yes	Packet loss is reduced.
10	Hangmei Deng et.al[10]	Modify RREQ and RREP	AODV	NS-2	Yes/Yes	Only detect the black hole attack but not the cooperative black hole attack.
11	Kaur Deng et.al[11]	Digital Signature	AODV	MATLAB	Yes/Yes	Reduced cooperative black hole attack.
12	Ayesh Siddiqua et.al[12]	Secure Knowledge Algorithm	AODV	NS-2	Yes/No	Help to find out reason before claiming node as a black hole node.
13	T.Manikandan et.al[13]	Modify RREQ,RREP and RERR	AODV	NS-2	Yes/No	Selective black hole node discovery process and performance analysis.

Conclusion

In this work, it has been concluded that decentralized and self-configuring network comes under the mobile ad-hoc network that makes it easy for malicious node to enter the network and makes it more prone to different active and passive attacks. In this paper, techniques have been reviewed which are used to detect blackhole attack in the network. The techniques have been reviewed in terms of certain parameters and description.

References

[1] Jydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detecting of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Second International Conference on Intelligent Systems ,Modeling and Simulation.IEEE-2011

[2] Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen, "Detecting Black hole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording", IEEE Wireless Communications, Vol. – 11 2010.

[3] H.A. Esmaili, M.R. Khalili Shoja, Hossein gharaee, "Performance Analysis of AODV under Black hole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT), Vol. 1, No. 2, pp. 49-52, 2011.

[4] Vaishali Mohite, Lata Ragha, "Cooperative Security Agents for MANET", IEEE World Congress on Information and Communication Technologies, pp. 549-554, 2012.

[5] Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

6] Osathanunkul, K.; Ning Zhang, "A countermeasure to black hole attacks in mobile ad hoc networks," IEEE International Conference on Networking, Sensing and Control (ICNSC), pp.508-513, April 2011.

[7] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Black Hole Attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[8] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, MAY 2008.

[9] Songbai Lu; Longxuan Li; Kwok-Yan Lam; Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", International Conference on Computational Intelligence and Security, vol.2, pp.421-425, Dec. 2009.

[10] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vol.40, no.10, pp. 70- 75, October 2002.

[11] Ravinder Kaur and Jyoti Kalra, "Detection and Prevention of Black Hole Attack with Digital Signature", International Journal of Advanced Research in Computer

Science and Software Engineering, Volume 4, Issue 8, August 2014.

[12] Ayesha Siddiqua, Kotari Sridevi, Arshad Ahmad Khan Mohammed, "Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm", Dept. of ECE, K L UNIVERSITY, SPACES-2015.

[13] T.Manikandan, S.Shitharth, C.Senthilkumar, C.Sebastinalbina, "N.Kamaraj, "Removal of Selective Black Hole Attack in MANET by AODV Protocol", Volume 3, Special Issue 3, March 2014.

[14] Jai Shree Mehta, Shilpa Nupur, Swati Gupta, "An Overview of MANET: Concepts, Architecture & Issues", International Journal of Research in Management, Science & Technology, Vol.3, No.2, April 2015.

[15] Ram Ramanathan and Jason Redi, "A Brief Overview of Ad Hoc Networks: Challenges and Directions", IEEE Communications Magazine-50th Anniversary Commemorative Issue/May 2002.

[16] Naeem Raza, Muhammad Umar Aftab, Muhammad Qasim Akbar, Omair Ashraf, Muhammad Irfan, " Mobile Ad-Hoc Networks Applications and Its Challenges", Communication and Networks, 2016.

[17] Ali Dorri, Seyed Reza Kamel, Esmail Kheyrkhah, "Security Challenges in Mobile Ad Hoc Networks: A Survey", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015.

[18] Y.Z.a and W. Lee, "Intrusion Detection in Wireless Ad-Hoc networks", presented at the 6th Int'l. Conf. Mobile Comp. Net., MobiCom, 2000.

[19] Yi-Chun, Adrian Peering, David B.Johnson, "Ariadne: A Secure on-Demand Routing Protocol for Ad Hoc Networks", sparrow.ece.cmu.edu/~adrian/projects/secure routing/Ariadne.pdf, 2002.

[20] Ms. Nidhi Sharmal, Mr.Alok Sharma, "The Black-Hole Node Attack in MANET", Second International Conference on Advanced Computing & Communication Technologies, 2012.