Educational Administration: Theory and Practice
2024, 30(6), 4194-4198
ISSN: 2148-2403
https://kuey.net/

Research Article

Prevention and Detection Methods of Black Hole Attacks– A Review

Ms. C. B. Banupriya[1*], Dr. S. Uma[2]

[1]Ph.D. Research Scholar, Department of Computer Science, C.M.S College Of Science and Commerce Coimbatore-49, Tamil Nadu, India
[2]Associate Professor, Department of Computer Science, Dr. N.G.P. Arts and Science College

Citation: Ms. C. B. Banupriya et. Al, (2024), Prevention and Detection Method s of Black Hole Attacks–A Review, Educational Administration: Theory And Practice, 4194-4198, Doi: 10.53555/kuey.v30i6.6535

ARTICLEINFO

ABSTRACT

A MANET is a continuous self-structured network in which mobile devices are connected wirelessly. The devices in MANET are free to move which pays way for the possibility of attacks. The possibility of attacks includes black hole attacks, grey hole, warm hole, and sinkhole attacks. A black hole referred as "hole of block" refers to an area where the incoming or outgoing packet is silently descended without informing the sender that the data does not reach its receiver and can only be detected by the traffic which is lost. This paper illustrates various prevention and detection methods for black hole attacks.

Keywords: MANET, Black hole, Data packet, AODV

1. NTRODUCTION:

MANET is a combination of wireless hosts that can be arranged easily as multiple packet networks without the help of infrastructure that is fixed or with the help of a centralized administrator [1]. The network architecture is classified into three types
[12]: Technologies that are enabled, Networking, Middleware, and its applications. To have a smooth communication, self-organized, dynamic, and volatile environment the main features of these networking protocols need to be re- created. The development of MANET has grabbed the attention of popular business manufacturing to a standard community.

1.1 ChallengesofMANET

The following is the list of defects that need to be overcome in the MANET environment [13].

- **Restricted Range of Transmission**: There must be a restriction in the wireless network which provides the result much overwhelmed than the bound network
- **Time-varying wireless link characteristics**: Characteristics such as path harm, and declining channel restrict the data rate and consistency
- **Packet Losses**: Packet damage such as unbearable bit error rate occurs in the wireless networks
- **Battery Restriction**: Usually Ad- hoc networks provide limited resources, so the nodes connected in these types of networks provide the inability in direction and node capacity.
- **Routing**: The main challenge in MANET tends to be routing. Due to drastic changes in network topology and mobility speeds, there arises a performance reduction in network nodes.**Security**: Another important challenge in MANET is its security because the data between the nodes can move freely.
- **Quality of service**: Mobility of nodes, node deployment, lack of coordination, resource constraints, and topology changes make quality of service very challenging.

1.2 Important Parameters in MANET Security:

MANET has special characteristics such that it has its metrics for security which are simply called “Security Parameters”. The parameters in MANET security are as follows:
Network Overhead: This parameter refers to the number of control packets generated by the security approaches
Processing time: Each security mechanism must focus on processing to enhance its features. Because of the dynamic topology of the MANET, there is a possibility of breakage of nodes and hence it is necessary to have low processing time to enhance flexibility.

Energy Consumption: MANET nodes have a limited energy supply so consumption of energy is an extremely challenging task. The high amount of energy consumption leads to node lifetime reduction.

1.3 Security Services:

Security service aims to secure the network before the attack occurs. The MANET should provide the services one by one and guarantee every service. Here we discuss the important security services.
Authentication: As the name indicates its hould "authenticate" which means the node should not have any doubt about the sender. For this purpose, several key certifications are used. The distribution of keys and management of keys is challenging.
Availability: Every node in the network should have access to all the services in the network. The challenge here arises because of the dynamic topology of MANET.
Data Confidentiality: As per this each node has permission to access the service, but the challenge here arisesdue to the central management of MANET.
Integrity: It refers to the services that only authorized nodes can modify, edit, and delete packets
Non-Repudiation: It is a type of service that ensures that the data sent by a node is repudiated by another node and can't deny it.
Some of the reasons for MANET being unsafe include No central Management, Freedom for a node (any node can freely enter), Low power, Trust issues using routing protocols, and at last loss of data during transmission. The attacks in MANET include the Black hole attack, Wormhole attack, snooping attack, Routing attack, denial of service, Jamming attack, etc. This paper illustrates black hole attacks and some of the prevention and detection methods used as of now.

2. BLACKHOLE ATTACK

It is a type of attack in MANET in which a malicious node attracts the data packets by sending a false path to the destination. It absorbs or takes the data packets and doesn't forward the packet to the destination. In some cases, malicious nodes work as a team [1].

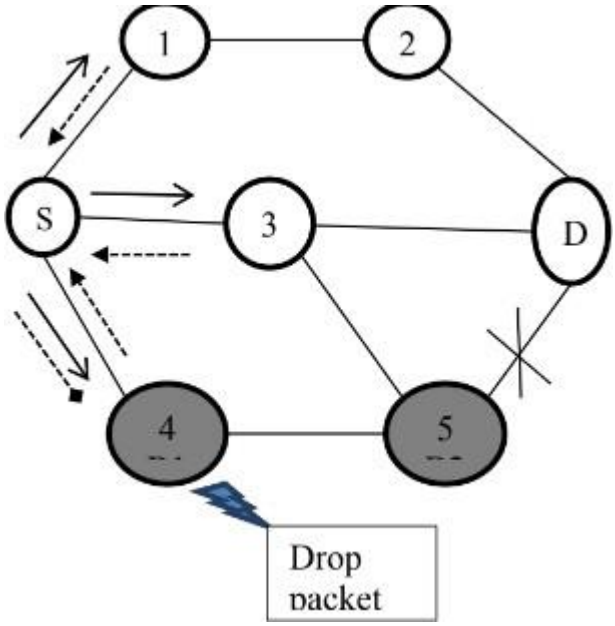

Figure1: Blackholeattackin network

Figure 1 shows a black hole attack which is fired. Here S tends to be the source node and D serves as the destination node. The intermediatory nodes(4) and(5) which are in the group act as black hole nodes. When the source node needs to send data to the destination it sends a request message to the nearest nodes. The malicious nodes receive this and send a reply message to the source node. After receiving thereply message, the source node sends data continuously which is received by the malicious node. It drops it and does not send it to the destination.

3. RELATED WORK

Sen et al. [1] proposed a method for detecting black hole attack in MANET. They used two concepts to modify the AODV protocol. One is DRI (data routing information) and the other one is cross- checking. Every node maintains a DRI table which consists of information such as value that is either true or false. Cross-checking uses the DRI table to send requests to the intermediatory nodes. By using this mechanism delivery ratio is increased but the overall performance is decreased [1].

Ren et al. [2] proposed a technique to detect black hole attacks using packet recording of packet exchange in networks. Here two tables are used. One is called RRT (receiving record table) and SRT(self-record table).RRT is used for reply messages and SRT is used for request messages. This technique provides a high detection rate and a low positivity rate.

Esmaili et al.[3] proposed a scheme to detect the performance of AODV protocol by using a simulator calledopen network, which comes under black hole attack. This paper uses two approaches to secure MANET. One is securing the routing of ad-hoc using routing protocols such as DSR(dynamic state routing), DSDV(Destination sequence distance vector), and two other protocols. Another one is the Intrusion detection system which provides next- hopinformationwithreplymessages.By using this approach packet delivery ratio is increased but it reduces in case of black hole attack

Mohite et al. [4] suggested a mechanism to detect black hole attacks in groups by usingcooperativesecurityagents. It uses 3 mechanisms. One is a self-record table and receiving record table as proposed earlier and the second one is routing informationofdataandthethirdconcept iscooperativesecurityagents.Byusingthese 3 methods the negative impact of attacks are somehow reduced.

Osathanunkal et al. [5] suggested a mechanism called S_ETX (secure expected transmission count). It is an extended version of the expected transmission count. It performs two modifications.oneisthedranddfvalues which are calculated by the initiator and the other one is to note which packetsare received which is the work done by the initiator. By using this performanceis increased and also at the same time, the cost overhead is reduced.

Raj et al. [6] proposed Detection, prevention, and Reactive AODV to detect and prevent the black hole attack. In this method when the AODV receives a replyit checks the sequence number of the node. If the sequence number seems tobehigherthanthevalueofthresholdit is claimed as a harm node and sends the ALARM packet to the neighboring nodes. By using this delivery ratio is increased, and routing overhead is normalized, but the traffic overload increases.

Tamilselvan et al.[7] proposed a mechanism to seclude the black hole attacks by using the concept of a fidelity table which means it keeps track of the fidelity level of nodes. If it is less than the threshold value it is declared as a Malicious node. It increases the delivery mechanism of the packet but at the same time increases the overhead.

Lu et al. [8] suggested the Secure AODV(SAODV) protocol to provide more security by routing the discovery process. By making use of this protocol the packet loss is reduced to 8.312%Kaur et al. [9] proposed a verification technique called “digital signature “to detect and prevent black hole attacks. It uses a TTL (time to live) scheme to choose the shortest path from different nodes. It uses a signature column at the destination node to note down the visiting nodes. It is used in preventing the black hole attacks in the group.

Siddiqui et al. [10] proposed a knowledgealgorithmwhichissecuredto prevent black hole attacks in MANET. Here every node monitors the neighboring nodes and compare the information with the knowledge table. If the fm and rm values in the knowledge table do not match it is treated as a maliciousnode.Themainsuccessofthis is that it finds the packet drop reason beforeclaimingthenodeisattacked bya black hole.

Manikandan et al. [11] proposed a scheme to remove the selective black hole attack in MANET by using the reacting protocol as AODV. This refers to an attack by a node which is harmful that produces a false sequence number and hop counting of the routingmessage. It uses three mechanisms description of the protocol, discovery process, and performance analysis.

Thecomparativeliteraturereviewhas been presented in Table 1

Table1: LiteratureReviewforDetectionandPreventionof BlackHole Attack

S.no	Author	Nameofthe Paper	MethodName	Prevention / Detection	Remark
1	Senetal. [1]	A mechanism for detection of Cooperative blackholeattack in MANET	DRI table and cross-checking	No/Yes	Increases the packetdelivery ratio by 17% but performance is decreased
2	Renetal. [2]	Detecting black hole attacks in Disruption tolerantnetwork through packet exchange Recording	RRTandSRT tables	No/Yes	Highdetection rate and low preventionrate
3	Esmailiet al.[3]	Performance Analysis of AODV under black hole throughtheuse of OPNET simulator	Securead-hoc routing and Intrusion detection	No/Yes	Packetdelivery is reduced in thepresenceof a black hole attack.

4	Mohiteetal. [4]	Co-operative SecurityAgents for MANET	Co-operative SecurityAgents	No/Yes	Detection is effective and reduces the negativeimpact of the black hole attack
5	Osathanunkal et al.[5]	A countermeasure to black hole attacks in MANET	SETEX Protocol	No/Yes	Performance is increased and costoverheadis reduced.
6	Rajet al.[6]	A dynamic learningsystem against black hole attack in AODV-based MANET	DPRAODV: Solution against blackholeattack	Yes/Yes	The packet deliveryratiois increased and normalized routing overhead
7	Tamilselvan et al.[7]	Prevention of Co-operative blackholeattack in MANET	Prevention of Cooperative blackholeattack in MANET usingfidelity table	Yes/Yes	The packet deliveryratio increases
8	Luet al.[8]	SAODV-A MANET Routingprotocol that can withstand black hole attack	SecureRouting Protocol - SAODV	Yes/Yes	Packetlossis reduced
9	Kauretal.[9]	Detectionand Preventionof black hole attacks using digital signatures	Digital Signature	Yes/Yes	Reduced cooperative black hole attacks.
10	Siddiqui et.al[10]	Preventingblack hole attacks in MANET using Secure Knowledge Algorithm	Secure Knowledge Algorithm	Yes/No	Helps to find out the reason beforeclaiming the node as a blackholenode
11	Manikandan et al.[11]	Removal of selectiveblack hole attack in MANET by	ModifyRREQ, RREP, and RERR	Yes/No	Black hole discovery processand analysis

4. CONCLUSION

A black hole attack is a type of attack in MANET that is to dissolve or to be listened to in the message during routing discovery. Security is the main concern in MANETs. Due to distinctive properties such as dynamic topology, limited resources, and shared medium, MANET are exposed to attacks. The black hole node sends a false reply and gets the information from the source node. This paper describes various methodsforthedetectionandpreventionofblack hole attacks by using various methods and techniques. The methods listed here are used to keep safe against black hole attacks. So, future work is intended to develop a more advanced security algorithm that will try to prevent and detect malicious nodes.

REFERENCES

1. J.Sen,S.KoilakondaandA.Ukil,“AMechanism for Detection of Cooperative Black Hole Attack in MobileAdHocNetworks”,inProceedingsof2nd InternationalConferenceonIntelligentSystems,Modeling,andSimulation,pp.338-343,2011
2. Y. Ren, M. C. Chuah, J. Yang and Y. Chen, "Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording", in Proceedings of IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM), pp. 1-6, 2010.
3. H. A. Esmaili, M. R. KhaliliShoja, Hosseingharaee, “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. V. Mohite and L. Ragha, “Cooperative Security Agents for MANET”, IEEE World Congress on Information and Communication Technologies, pp. 549-554, 2012.
5. K. Osathanunkul, and N. Zhang, "A countermeasure to black hole attacks in mobile adhoc networks”, IEEE International Conference on Networking, Sensing, and Control (ICNSC), pp.508- 513, April 2011.
6. P.N.RajandP.B.Swadas,“DPRAODV:ADynamic Learning System against Black HoleAttack in AODV based MANET”, IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.
7. L. Tamilselvan, V. Sankaranarayanan, “Prevention of Co-operative Black Hole Attack in MANET”,JournalofNetworks,Vol.3,No5,13-20,2008.
8. S.Lu,L.Li,K.Y.Lam,andL.Jia,"SAODV:AMANETRoutingProtocolthatcanWithstandBlackHole Attack", International Conference on Computational Intelligence and Security, Vol. 2, pp. 421-425, 2009.

9. R. Kaur and J. Kalra, "Detection and Prevention of Black Hole Attack with Digital Signature", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 8, 2014.
A. Siddiqua, K. Sridevi, A. A. K. Mohammed, "Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm", In Proceedings of International Conference on Signal Processing and CommunicationEngineeringSystems(SPACES),pp. 421-425, 2015
10. T. Manikandan, S. Shitharth, C. Senthikumar, and C. Sebastinalbina, "Removal of Selective Black Hole AttackinMANET byAODV Protocol",Vol. 3, No.3, 2014.
11. J. S. Mehta, S. Nupur, and S. Gupta, "An Overview of MANET: Concepts, Architecture & Issues", International Journal of Research in Management, Science & Technology, Vol. 3, No. 2, 2015.
12. N. Raza, M. U. Aftab, M. Q. Akbar, O. Ashraf, and M. Irfan, "Mobile Ad-Hoc NetworksApplications and Its Challenges", Communication and Networks, Vol 8, No. 3, pp. 131, 2016.
13. A. Dorri, S. R. Kamel, and E. Kheyrkhah, "SecurityChallengesinMobile Ad Hoc Networks: A Survey", International Journal of Computer Science &Engineering Survey(IJCSES) Vol. 6, No.1, pp. 15- 29, February 2015.