ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

A Survey on Discovery and Prevention of Black-Hole Attack in WSN

Kashyap Dave[1], Prof. Wasim Ghada[2]

M.E. Student, Dept. of Computer Engineering, B.H.Gardi college of Engi. & Tech., Rajkot, Gujarat, India[1]

Assistant Professor, Dept. of Computer Engineering, B.H.Gardi college of Engi. & Tech., Rajkot, Gujarat, India[2]

ABSTRACT: Wireless Sensor Networks (WSN) is a rising innovation now-a-days and has an extensive variety of uses for example traffic surveillance, forest fire detection, battlefield surveillance, flood detection etc. but WSN can be affected by various attacks which obstructs ordinary operation of the system. Security and reliability of sensor network is less because of arbitrary architecture of sensor nodes in open environment, power limitations, memory limitations and unattended nature.Generally, two types ofAttacks are in WSN- active attacks and the passive attacks. Black-hole attack is injurious active attacks. In this review paper we have reviewed some technique which are for discovery and prevent black-hole attack.

KEYWORDS: WSN; Black-hole attack; discovery; prevention mechanism;

I. Introduction

A WSN is collection of numbers of sensor nodes which are distributed in environment. This allows random distribution of nodes in inaccessible terrains, disaster relief operations and some other applications. Other applications of WSN are environmental control such as fire-fighting or installing sensors on bridges or buildings to understand earthquake vibration patterns also marine ground floor erosion, surveillance tasks etc. Due to infrastructure less environment and wireless nature of WSN, they are more affected by many types of security attacks.

There are several types of attacks can be done by malicious nodes to damage the network and make that network unreliable for communication and proper working. Some of such kinds of attacks are:

a) *Wormhole Attack:* In wormhole attack attacker records packets at one place and tunnels those to another place in network. Due to this itcreates False scenario that main sender is neighbor of remote location. Wormhole forms by tunneling procedure in sensor network.

b) *Tempering:* its tempers hardware configuration of sensor and gain physical access for making node as adversary node. Tempering can be done at physical layer.

c) *Jamming:* this attack is related with troublemaking or interfering radio frequencies which are used by sensor nodes. By gating physical access of some nodes attacker can create jam in network to disturb the network.

d) *Sybil Attack:* In Sybil attack a malicious node illegally take multiple identities. In this an adversary can appear in multiple places at the same time. A node presents multiple identities to other nodes in network by stealing or fabricating the identities of authenticated nodes. This attack is done on network layer.

e) *Hello Flood Attack:*Its uses HELLO packets as a weapon to convince the sensors in WSN. In this attack an attacker have high radio transmission range and processing power. They sends HELLO packets to number of sensor nodes which are in a large area within a WSN.

f) *Black hole Attack :*In the black-hole attack, advertises of the wrong paths as good paths to the source node by a malicious node during the path finding process as in reactive routing protocols or in the route updating messages as in proactive routing protocols.[1]

DOI: 10.15680/IJIRCCE.2015. 0310040

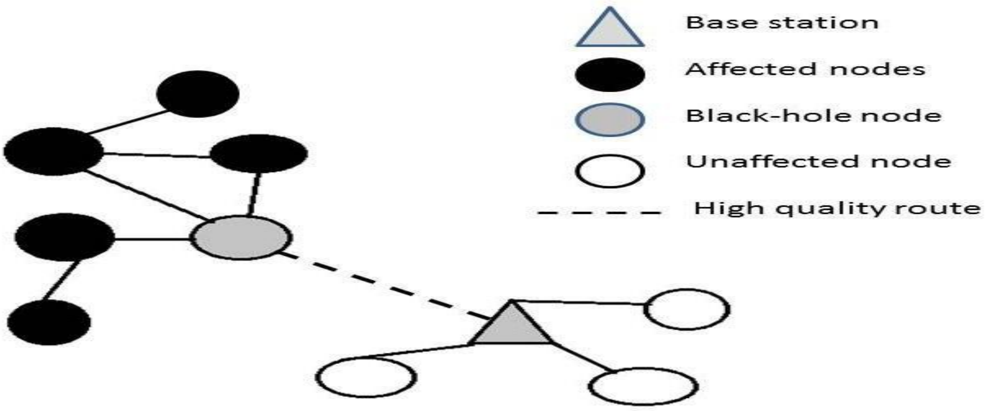

Fig. 1 Black hole Attack [1]

Black hole attack are of two types:

- *Single Black Hole Attack*: only one node act as malicious or cooperated node which misbehavior with the network in Single black hole attack. It is also known as black hole attack with single malicious node.
- *Collaborative Black Hole Attack:* multiple nodes behaves as malicious node in the network and works in co-operative manner in Collaborative black hole attack. Also known as black hole with multiple malicious nodes.

II. RELATED WORK

Sr. No	Paper Name	Author	Publication Year	Description
1	detecting black hole attack in wsn by check agent using multiple base stations[1]	SwarnaliHazra and S.K. Setua	2013	Detects black hole attacker in entire network.in that high detection rate as shown in simulation result. Their proposed trust computation and trust model define trust level of relationship between nodes in network. One node believes or disbelieves its trustee depending on trust level. With disbelief of thruster, black hole attacker are detected and removed from route
2	Black hole attack defending trusted on-demand routing in ad-hoc network[3]	Harmandeep Sinh and Manpreet Sinh	2014	The effect of black hole in ad hoc wireless networks. They implemented an AODV protocol that Simulates behaviour of a black hole in NS-2. For this method they have used very simple and effective way of providing security in AODV against black hole attack that causes the interception and confidentiality of ad hoc wireless sensor networks. Their solution detects malicious nodes and removes it from the active data forwarding. As per graphs showed in result they easily conclude that performance of the normal AODV drops under the presence of black hole attack

3	securing MANETs routing protocol under black hole attack[4]	M. Mohanapriya and IlangoKrishnamurthi	2014	That is simple acknowledgement scheme to detect Black hole nodes in MANET. It can be incorporated with any existing on demand ad hoc routing protocols. By their proposed algorithm, destination node detect the presence of malicious node in the source route and with the help of intrusion detection system the malicious nodes are removed from the network. Their IDS nodes resulting less energy loss, which makes their method suitable for the resource constrained characteristics of MANET. By simulation results percentage of data packet loss in their proposed work is better than DSR in presence of multiple grayhole nodes.
4	Modified DSR protocol for detection and removal of selective black hole attack in MANET[5]	SatyajayantMisra and GuoliangXue	2011	BAMBi:Black hole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. That effectively mitigate the effect of black hole attack on WSNs. It's based on deployment of multiple base stations in the network and routing of copies of data packets to that base stations. Their solution is highly effective and require very little computation and message exchanges in the network, so saving the energy of the SNs.
5	Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks[6]	AbderrahmaneBaadache and Ali Belmehdi	2014	An authenticated end-to-end acknowledgment based approach that checks correct forwarding of packets by intermediate nodes. Their approach detects the black hole launched in simple or cooperative manner. No modification and the no reply of messages are required to fully deliver the message to the destination node. Compared to 2-hop ACK and watchdog approach, their approach has best delivery ratio of packet and the highest detection ratio.
6	Elimination of black hole and false data injection attacks in wireless sensor networks[7]	R. Tanuja and M. K.Rekha	2013	A new acknowledgement based detection scheme which helps to simplify the removal of black holes and guarantees successful delivery of packets to destination. Their algorithm can successfully identify and eliminate 100% black hole nodes and ensures more than 99% packet delivery.
7	A force routing information modification model for preventing black hole attacks in wireless ad hoc network[8]	Muhammad Raza and Syed IrfanHyder	2011	FRIMM (A Forced Routing Information Modification Model). It's applied on AODV protocol. It is constructed on three basic devices such as server, access points and nodes. They used WiMax technology for communication between server and access point, other technology WiFi for the

				communication between access point and node. Node do not direct communicate with server. If malicious node communicate with node as server than access point will fetch MAC address of malicious node. Server will attack the black hole by introducing jamming style and eliminate that node from the route and diverts its traffic towards access point.
8	Application of formal modeling to detect black hole attack in wireless sensor network routing protocols[9]	KashifSaghar and David Kendall	2014	RAEED (Robust formally Analyzed protocol for wirEless sEnsor networks Deployment) is developed routing protocol. Which is able to address the problem of black hole attacks using formal modeling and proves that RAEED avoids such kind of attacks.
9	CAODV Free Black hole Attack in Ad Hoc Networks[13]	WatcharaSaetang and SakunaCharoenpanyasak	2012	By using credit mechanism, they detect and protect malicious node before blackhole attack is occurred. Blackhole cannot attack the networks when CAODV is employed. With CAODV average throughput of original AODV id decreased about 40% during blackhole attack.
10	Security against black hole attack in wireless sensor network – A Review[14]	Binod Kumar Mishra and Mohan C. Nikam	2014	They will prepare lightweight security model which validate the sensor node and then allow transmit true information to the base station.
11	Detection and Defense Technology of Blackhole Attacks in Wireless Sensor Network[16]	HuishengGao, Ruping Wu	2014	In proposed technique detection and prevention of blackhole attack to reduce the possibility of selecting a path having blackhole nodes in the route discovery process. This technique works effectively for analysis and defines blackhole attack
12	Impact of Blackhole and Rushing Attack on the Location Based Routing Protocol for Wireless Sensor Networks[17]	R. Shyamala , S. Valli	2012	Here effect of blackhole attack and rushing attack studied for GMR protocol. The throughput, packet delivery ratio, energy loss and end to end delay have been evaluated. They reduced end to end delay, throughput and packet delivery ratio.
13	Acknowledgement-Based Trust Framework for Wireless Sensor Networks[18]	X. Anita, J. Martin Leo Manickam	2014	Here 2-ACKT-1 is proposed trust based evaluation framework. They showed that their protocol has better performance as compare to conventional multihop and trust based routing protocol for control overhead, packet delivery ratio and network life time. Malicious attackers are revealed by individual sensor node.

14	Securing data from blackhole attack using AODV routing for mobile ad hoc networks[19]	V. Kamatchi and R. Mukesh	2013	In this paper using random dispersive routes extreme throughput is accomplished with reduced delay even after blackhole occurrence. Energy consumption is reduced at both sender and receiver and high security is reached. With the Minimal energy factor communication between sender and receiver is achieved.
15	TBESP Algorithm for Wireless Sensor Network under black hole Attack[20]	M. Wazid, A. Katal and R. Goudar	2013	In this paper authors observed that if network is blackhole prone and want throughput efficient service then we have to select Mesh topology in place of tree topology. If we want time efficient service then we have to go for Tree topology in place of Mesh topology. Depending upon these results the TBESP algorithm is proposed which efficiently chooses the required topology as per the network service requirement.
16	Effect of Blackhole Attack on Single Hop and Multihop Leach Protocol[21]	S. Iqbal, A. Srinivas , G. Sudarshan and S. Kashyap	2014	In this paper we are giving simulation results to information transmitted, number of alive hubs and comparing so as to linger vitality single bounce LEACH, multi jump LEACH and the impact of Black hole assault on them. The information transmitted is minimum in the multi jump LEACH system influenced by Black hole assault and most extreme in the system of single jump LEACH without assault.
17	Intrusion Detection in Wireless Sensor Networks[22]	M. Krishnan	-	SPINS, Maintaining Service Availability, Sleep Scheduling this protocols are used, as well as some ways to determine where to check packets, including a new game theoretic approach in which we saw that by allowing the attack to have some utility, we are able to increase ours through energy saving for sufficiently large, resource constrained networks.

Table 1: Survey Table

III. Comparison

Sr. No.	Technique	year	Routing protocol Used	Simulation tool	Performance matrix	Result
1	Trust on demand [2]	2014	AODV	NS2	Packet loss	Packet loss decreases
2	Enhanced AODV [3]	2013	AODV	NS2	Packet delivery ratio, Average End-to-End Delay, throughput	Increase packet delivery ratio and throughput and decrease Average End-to-End delay
3	MDSR[4]	2013	DSR	NS2	Packet drop ratio,	Reduce packet drop

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

					overhead, End to end delay	ratio and end to end delay , increase overhead
4	BAMBi [5]	2011			Packet delivery ratio , detection ratio	About 99% packet delivery ratio, 100% detection ratio
5	authenticated end-to-end acknowledgment based approach[6]	2014	AODV , OLSR	OPNET modeller	End to end delay, network load	Decrease end to end delay, increase network load
6	False data injection[7]	2013	MAC	MATLAB	Packet delivery rate	Increased packet delivery rate
7	FRIMM[8]	2012	AODV	-	-	-
8	RAEED[9]	2014	INSENS	TOSSIM	% of node blocked	Robust and low overhead
9	WBACA[10]	2005		GloMoSim	Reaffiliations , starting delay	Reaffiliations increase, starting delay decreased
10	Detection technique based on routers[11]	2013	-	-	End to end delay , throughput	Decrease end to end delay, increase throughput
11	CAODV[13]	2012	AODV	NS2	throughput	Increase throughput
12	Detection technique[15]	2013	AODV	NS2	Packet delivery ratio, delay , overhead	Packet delivery ratio increased, delay reduced, overhead reduced
13	DSN based	2015	AODV	NS2	Throughput , end to end delay	Increase throughput , decrease end to end delay
14	Geostatistical based	2014	AODV	OMNET++	False positive , False negative	Adopted 95% confidence level
15	MDSR	2013	DSR	GloMoSim	Packet drop ratio, end to end delay, PDR, overhead	Percentage of packet loss rate is better

Table 2: Comparison

IV. CONCLUSION AND FUTURE WORK

In this paper I have reviewed many technique which are used for detection and prevention of black hole attack. Different techniques that we have reviewed are detecting and preventing black hole attack along with that improving performance matrices. Increasing packet delivery ratio, throughput also decreases End-to-End delay, overhead. After comparing all this techniques I conclude that BHnFDIA is efficient technique for detecting black hole attack it gives 99% packet delivery ratio, 100% detection ratio.

REFERENCES

1. NiteshGondwaland ChanderDiwaker,'detecting blackhole attack in wsn by check agent using multiple base stations', American International Journal of Research in Science, Technology, Engineering & Mathematics, 2013.
2. SwarnaliHazra and S, K. Setua,'Blackhole attack defending trusted on-demand routing in ad-hoc network', Springer , advance computing, networking and informatics – vol 2, 2014.
3. Harmandeep Singh and ManpreetSingh,'securing MANETs routing protocol under blackhole attack', International Journal of Innovative Research in Computerand Communication Engineering – Vol 1, issue 4 , june 2013
4. M. Mohanapriya and IlangoKrishnamurthi, 'Modified DSR protocol for detection and removal of selective black hole attack in MANET', ELSEVIER, 2014.

5. SatyajayantMisra and GuoliangXue , ‘ BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks’ , IEEE 2011.
6. AbderrahmaneBaadache and Ali Belmehdi, ‘Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks’,ELSEVIER 2014.
7. R. Tanujaand M. K. Rekha,‘Elimination of blackhole and false data injection attacks in wireless sensor networks’, Springer science 2013.
8. Muhammad Raza and Syed IrfanHyder , ‘ A force routing information modification model for preventing black hole attacks in wireless ad hoc network ‘ , IEEE 2011.
9. KashifSaghar and David Kendall , ‘ Application of formal modeling to detect black hole attack in wireless sensor network routing protocols‘ , IEEE 2014.
10. Snajay Kumar Dhurandher and G. V. Singh, ‘Weight Based Adaptive Clustering in Wireless Ad Hoc Network ‘, IEEE 2005.
11. Mohammad Wazid andAvitaKatal,‘Detection and prevention mechanism for blackhole attack in e=wireless sensor network ‘, international conference on communication and single processing, 2013.
12. Chakchi So-In and KanokpornUdompongsuk, ‘performance evaluation of LEACH on cluster head selection techniques in wireless sensor network’, Springer 2013.
13. WatcharaSaetang and SakunaCharoenpanyasak, ‘CAODV free Blackhole attack in ad hoc networks’, International Conference on Computer Networks and Communication Systems, 2012.
14. Binod Kumar Mishra and Mohan C. Nikam, ‘Security against blackhole attack in wireless sensor network – A Review’, IEEE 2014.
15. S. A. Arunmozhi and Y. Venkataramani, ‘Black Hole Attack Detection and PerformanceImprovement in Mobile Ad-Hoc Network’ , ISJ 2012
16. HuishengGao, Ruping Wu, ‘Detection and Defense Technology of Blackhole Attacks in Wireless Sensor Network’, SPRINGER 2014
17. R. Shyamala , S. Valli, ‘Impact of Blackhole and Rushing Attack on the Location Based Routing Protocol for Wireless Sensor Networks’,SPRINGER 2012
18. X. Anita, J. Martin Leo Manickam, ‘Acknowledgement-Based Trust Framework for Wireless Sensor Networks’, SPRINGER 2014
19. V. Kamatchi and R. Mukesh, ‘Securing data from blackhole attack using AODV routing for mobile ad hoc networks’, SPRINGER 2013
20. M. Wazid, A. Katal and R. Goudar, ‘TBESP Algorithm for Wireless Sensor Network under black hole Attack’, IEEE 2013
21. S. Iqbal, A. Srinivas , G. Sudarshan and S. Kashyap, ‘Effect of Blackhole Attack on Single Hop and Multihop Leach Protocol’, IJERA 2014
22. M. Krishnan, ‘Intrusion Detection in Wireless Sensor Networks’

BIOGRAPHY

Kashyap Dave is a ME student in the Computer Engineering Department in B.H. Gardi college of engineering & Technology, Rajkot, Gujarat, India. He received Bachelor of Information Technology degree in 2014 from Noble Engineering College, Junagadh, Gujarat, India. His research interests are Computer Networks (Wireless Networks), Data mining,cloude etc.

Wasim Ghada is an Assistant Professor with more than 5 years teaching experience. He is assistant professor of Computer Engineering Department in B.H. Gardi college of engineering & Technology, Rajkot, Gujarat, India. He received Master of Engineering in computer engineering from Nirma University.