Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Black Hole Attack Detection and Prevention Schemes in Wireless Sensor Network

Aparna U. Chaudhary
M.E. (CE) II Year
PRMCEAM, Amravati,
Maharashtra, India

Prof. Priti A. Khodke
Assistant Professor
PRMCEAM, Amravati,
Maharashtra, India

Prof. A. U. Chaudhari
Assistant Professor
PRMIT&R, Badnera,
Maharashtra, India

Abstract— Wireless sensor networks are the most popular network now days. It has diverse field of application which is prone to the security threats. There is fast increment in threats of attack that creates terrible problems in the network. Black hole attack is one of the security threats, in which a malicious node is occurred, which absorbs all of the data packets towards itself. That's why all data packets are dropped in that network which result in misbehaving as well as damaged node interface. For such attacks there are various types of schemes to defend over them. In this paper, we review some research paper based on black hole attack, their detection and prevention schemes, security challenges, routing protocols etc. also we discuss about Black hole attack and their types.

Keywords— wireless sensor network, black hole attack, routing protocols.

I. INTRODUCTION

Network is a combination of nodes, where every node has its own specified work. The wireless Sensor Network (WSN) is also a combinational network where every node has predefined work to do. In WSN, Sensor node is known as mote. Because of its size and its usage, it is used everywhere, so that goal has to be achieved. Sensor nodes are frequently used at any place because of its size and its cost. It uses less memory and power to process the data.

The WSN is the infrastructure less network which is shown in fig.1. In which five mobiles are connected by the wireless link in that network. Where every node initiates route discovery process with the help of route request and route reply packets. By the use of routing protocol the infrastructure less network get managed. The consumption of energy is more for data communication than any other process. Secondary power source supply that yields power from the environment such as solar panels may be added to the node depending on the appropriateness of the environment where the sensor will be deployed.

WSN having various types of applications in different fields such as in military, medical, various industries, environmental monitoring, infrastructure monitoring, and many more. In this paper, various research papers which are based on WSN, Blackhole attack, its detection and prevention schemes and routing techniques are discussed.

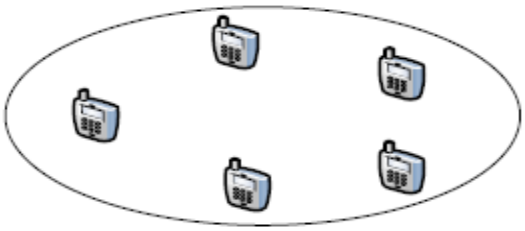

Fig.1. Infrastructure less Network

II. BLACK HOLE ATTACK

A. Overview

Black hole attack is a type of attack in network in which a malicious node uses the routing protocol of that network. That malicious node captures a node from that network and reprograms it that's why it doesn't transmit the data packets. That node absorbs all the transmission towards itself and fails to transfer over other node. The black hole attack possibly a node which drops the packets and transmit unwanted information because of its shortest path between source and destination. As a result the packets passed over the black hole region get captured and doesn't reach to the destination node. That causes delay in the delivery of the packet which reduces the throughput of network. Sometimes it is called as packet drop attack because in network it keeps on drop the attack. It is one of the serious attacks in the network. Generally this type of attack cause on specific protocols which prefers the device to broadcast like shortest path and access other devices.

The below fig.2 shows the how black hole problem arises in the network. In the above network consider node A is the sender and node D is the receiver. Node A has to send the packets of data to the destination node D and has to initiate the route discovery process. Suppose node C considered to be as a malicious node so that it shows active route to

the specified destination node. Eventually the node A will get the response from node C from this activeness of that node, node A will assume that this is the active route and will complete the active route discovery. From that node A makes the communication with node C and ignores all the replies coming from other nodes. That's why all the data packets get lost which result in destination node never communicate to the source node.

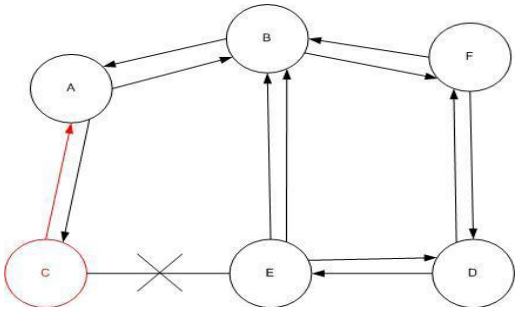

Fig.2. Blackhole problem

B. Types

There are two types of black hole attack those are as follows:

1. Internal black hole attack

The internal black hole attack having internal malicious node that fits in the given route of source to destination. After getting a chance that malicious node become an active data route element. Then it is capable of conducting attack with data transmission. The internal attack is more critical because of the internal misbehaving node.

2. External black hole attack

The external black hole attack does not include physically which creates congestion in the network. If the internal malicious node are not get controlled by the network then external attack will becomes internal attack.

III. ATTACKS ON WIRELESS SENSOR NETWORK

In WSN attacks are categorized into two different ways that are passive attack and active attack. In passive attack, attackers are acts as passive and it never distract the channel of communication. There is a data alternation possible in the active attack and it is very dangerous because network is not aware with the attack.

There are several types of active and passive attack found in the each layer ISO-OSI model which is shows in following table

TABLE I

Layers	Attacks	Security approaches
Physical layer	Denial of Service Tampering	Priority Messages Tamper Proofing Hiding, Encryption
Data link layer	Jamming Collision Traffic manipulation	Use Error Correcting Codes Use spread spectrum techniques
Network layer	Sybil attack Wormhole attack Sinkhole Flooding	Authentication Authorization Identity certificates
Transport layer	Resynchronization Packet injection attack	Packet Authentication
Application layer	Aggregation based attacks Attacks on reliability	Cryptographic approach

IV. LITERATURE REVIEW

Ankur mishra et al [1] proposed a mechanism for identification of multiple black hole nodes cooperating as a group in ad hoc network. They proposed mechanism work and make modification over AODV protocol and also make use of the data routing information table (DRI) with 'check bit' in addition to cached and current routing table. In MANET one of the reactive routing protocols is AODV protocol on which they are mostly focusing.

Sheela.D et al [2] proposed a system which is designed to defend against black hole attack by using multiple base stations deployed in network with the help of mobile agents. They are introducing black hole attack, multiple base station and mobile agent initially in that paper. The unnecessary transmission of packets to multiple base stations is to be avoided by detecting the abnormal behavior of certain nodes is followed upon which the data transmission to multiple base stations is triggered. For this purpose they make use of mobile agents which keep visiting the stationary nodes to detect any abnormality in the presence of black holes. Also they term the re-programmed nodes as black hole nodes and the region that containing the black hole nodes as a black hole region which is the entry point to a large span of insidious attacks. The simulation result will show the performance of proposed approach.

Shiva Murthy G et al [3] proposed a protocol which is a secure Energy Efficient Node Disjoint Multipath Routing protocol (EENDMRP). EENDMRP is a sink initiated proactive protocol. On the basis of the rate of energy consumption and length of the filled queue of that node EENDMRP protocol recognized the multiple paths between the source and destination. In this paper, they introduce public key cryptography in WSNs. The public key encryption technique uses pair of an asymmetric-key: a public key and a private key. Also they discuss on the working of EENDMRP having two phases route construction phase and data transmission phase.

Asmae Blilat, Anas Bouayad, Nour el houda Chaoui, Mohammed El Ghazi [4] proposed challenges for wireless sensor network security. In which they introduce different types of challenges and attackers goals for sensor network. Sensor network having some unique properties e.g., tree-structured routing, aggregation, in network filtering, etc., which having important security implications. Also they are discussing about the eavesdropping, traffic analysis, Disruption, Hijacking and Physical Attacks.

S. Kumar and S. Jena proposed (SCMRP) [5] which is a cluster base multipath routing protocol. The SCMRP model provides security against various attacks and in routing; there is use of effective key management technique like unique pair wise key distribution. The SCMRP model communicates with NeighBouR DETection (NBR DET) packet to construct the neighbor list in each node.

Marjan Radi et al [6] introduce a Low-Interference Energy-Efficient Multipath Routing protocol (LIEMRO) for WSNs. This model is a source initiated event-based, reactive routing protocol. The LIEMRO model is used to find the multi-path between the source and destination. However, the multipath which is introduced by this model excludes the node disjointedness property.

Choon-Sung Nam et al [7] proposed a scheme i.e. efficient path set up and recovery by using routing table in WSNs. With the help of routing table sensing data can be easily transfer from one node to another. That make efficient path establishment for the data transmission. Also this scheme satisfies the criteria that include robustness of data path failure.

Ke Guan et al [8] proposed an energy-efficient multi-path routing protocol for WSNs. In which they construct routing trees such as search tree and query tree. This routing protocol has three phases that are double routing tree construction, route discovery, and data transmission. The route discovery mechanism finds the multiple paths in between the source and the destination using shared nodes in the query tree and search tree.

M. Marina and S. Das [9] proposed a protocol for mobile ad hoc networks. They are using ad hoc on demand multipath distance vector (AOMDV) protocol that provide fault tolerance and efficient recovery from route failure in dynamic networks. The protocol computes multiple loop-free and link-disjoint paths. Multipath on-demand protocols try to alleviate these problems by computing multiple paths in a single route discovery attempt.

Nils Aschenbruck [10] proposed for WSNs security architecture and modular intrusion detection system. Monitoring of animals or humans or their surveillance, infrastructure, or territories had been involved in the application scenarios of WSNs. Since security as well as privacy is very important in these contexts, specifically the sensor nodes and networks should be protected from extreme environmental condition and malicious attacks. They proposed modular IDS as a framework for this architecture. Where the detection modules run on the motes and locally detect an attack. In case of detection, an alarm message is sent to the IDS server where the corresponding server-side module processes the message and the alarm is displayed in a GUI for immediate response.

Rutvij H. Jhaveri [11] investigate more existing mechanisms and propose a slight modification to RAODV that attempt to reduce further rise in normalized routing overhead. Also the article proposed a modification to AODV protocol to introduce security aspect into it.

Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic [12] proposed a concept of pair wise and triple key distribution in wireless sensor networks along with their applications. In the triple key distribution the three nodes shares common keys. Also they discuss about the application in secure forwarding along with the detection of malicious nodes and key management in clustered sensor networks.

Nikolaos A. Pantazis et al [13] proposed a survey on energy efficient routing protocol. Also they are classified into four main categories: Network Structure, Communication Model, Topology Based and Reliable Routing Schemes. They allow a section in which real deployment in WSNs and energy consumption in WSNs include. In this paper, they concentrate on the energy efficient protocols that have been developed for WSNs. They classify them in flat, hierarchical, query-based, coherent and non- coherent based, negotiation-based, location-based, mobile agent-based, multipath-based, QoS-based.

Anri Kimura et al [14] proposed a new multipath routing method, which reduces joint nodes from various multiple paths with few control packets while managing the maximum degree of connectedness, which is defines as the total number of paths connecting to a node, on the joint nodes. In which they used other than DART routing technique, that is new multipath routing method which helps in the reduction of the number of joint nodes on multiple paths. Where they are introducing two new values those are joint count and connectedness. From these they are improving the resilience against the node capture attack.

TABLE II

Ref No.	Author	Year	Basic concept	Performance evaluation	Our findings
1.	A. mishra, R.Jaiswal and S.sharma	2013	Detection and Elimination of Cooperative Black	effective in detection and elimination of the attack which maximizes network performance	Good performance compared to

			Hole Attack by using Advanced DRI Table in Ad hoc Network	by reducing the packet dropping ratio in networks	AODV
2.	Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M	2012	To defend against black hole attack using multiple base stations deployed in network by using mobile agents	lightweight, fast, efficient and the mobile agent technology based security solution defend against black hole attack in wsn	Mobile agents increases the life of system
3.	Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad	2012	Protocol for securing the disjoint nodes in multipath routing in wireless sensor networks using digital signature	Better results shown which measure in terms of packet delivery fraction, energy consumption, and end-to-end delay	Provides a simple way of securing WSN
4.	Asmae Blilat, Anas Bouayad, Nour el houda Chaoui, Mohammed El Ghazi	2012	Security challenges for WSN	Providing security to WSNs is very challenging	Wsn are not that much secure than other network
5.	S. Kumar and S. Jena	2010	It is an protocol that provide security while routing the cluster based multipath (SCMRP)	Provide security to the various network layer protocol attacks, also provide efficiency and the reliability to the networks	Cryptographic algorithm makes system secure
6.	M. Radi, B. Dezfouli, Shukor Abd Razak, Kamalrulnizam Abu Bakar	2010	Low-Interference Energy efficient Multipath Ruting protocol (LIEMRO) for WSNs	LIEMRO can make the construction of node disjoint path for each and every detected event. Also they evaluate LIEMRO in multiple event situations.	Multipath routing protocol increases efficiency
7.	K. Guan and L. M. He	2010	Energy efficient multipath routing protocol for wsn	Route discovery mechanism provides multiple paths present in the source and destination by using shared nodes in the query tree and search tree. This gives better performance than existing one.	Multipath routing is beneficial by all means
8.	M. Marina and S. Das	2001	On demand multipath distance vector protocol for mobile ad hoc networks	On-demand protocols achieve faster and efficient recovery from route failures in highly dynamic ad hoc networks	AOMDV is more efficient than AODV
9.	Nils Aschenbruc, Jan Bauer, Jakob Bieling, Alexander Bothe, and Matthias Schwamborn	2011	Security architecture and modular intrusion detection system in wsn	Identifying different well-known as well as WSN specific attacks on various layers	IDS as a framework for this architecture

Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari, Kumar Sidharth Choudhary [15] proposed a specification which is based on intrusion detection system which detects the black hole attack and the selective forwarding attack in wireless sensor networks. In which they are introducing an intrusion detection system along with perversion based technique and detection based technique. These specifications scan rule on the number of messages being dropped by a node.

Moh. Wazid, A. Katal, R. Singh Sachan, R. H. Goudar and D. P. Singh [16] proposed a mechanism of detection and prevention for black hole attack in wireless sensor networks. As we know a black hole attack are very difficult to detect and defend. In this mechanism they build cluster from sensor nodes. The election of cluster co-coordinators is done by sensor nodes. The cluster coordinators elections having two things to be considered that are fairness and efficiency. The algorithm that has been used is capable to detect and prevent the Black hole attack occurring in the WSN.

P. Chanak, I. Banerjee, H. Rahaman [17] proposed a technique for distributed multipath fault tolerance routing for wireless sensor networks (DFTR). In this scheme nodes are arranged in efficient size cluster and data is to be transmitted to different path with energy efficient manner. This technique is use cluster based fault tolerance routing. The architecture of multipath fault tolerance routing scheme having two phases those are effective size cluster formation and multipath data routing tree formation.

Madhu, Alpana Dahiya, Brahmprakash Dahiya [18] proposed a system for energy efficient data transfer in secure wireless sensor networks. In which they initially introduce the architecture of wireless sensor networks and the study of flooding algorithm and then remove limitation of flooding algorithm using grid network. From that they analyze Horizontal–Vertical method which performs better load balancing of the grid network.

Abhishek Jain, Kamal Kant, M. R. Tripathy [19] proposed security solutions for the wireless sensor network. They provide the information about the security requirements and also provide the identification and categorization of security threats. The main focus is to review and develop various securities schemes/solutions for wireless sensor networks.

Zhang Yu [20] proposed a scheme of public key infrastructure which improves the wireless sensor networks security. In which they are trying to solve the security problem by using public key cryptography which is serve as tool for authentication of base station. They provide the scheme of public key encryption in that symmetric encryption based schemes, public key based schemes, RSA scheme are introduced. Security analysis provide various security services and along with that development of the security.

Qian Yu and Chang N. Zhang [21] proposed a secure multicast scheme for wireless sensor networks. Without sacrificing the strength of security properties the sensor node can afford to implement secure multicast efficiently. This scheme composes group key management and data security.

V. CONCLUSIONS

The wireless sensor network has wide range of security attack due to its open and unprotected environmental area. In this paper we have reviewed different existing black hole attack detection techniques and their control measures. It has been studied that among the number of methods discussed, each of them having their own strength and weaknesses.

REFERENCES

[1] Mishra, R. Jaiswal and S.sharma, "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRITable," in Int. Advc. computing conf.(IACC) 2013 pp.499-504.

[2] Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M., "Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent, "in Int. Conf. on Art. Intelligence and Emb.Systems (ICAIES'2012) July 15-16, 2012 Singapore pp.45-48.

[3] Shiva Murthy G, Robert John D'Souza, and G. Varaprasad, " Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks, "in IEEE sensors journal, vol. 12, no. 10, October 2012, pp.2941-2948.

[4] Asmae Blilat, Anas Bouayad, Nour el houda Chaoui, Mohammed El Ghazi, "Wireless Sensor Network: Security challenges", IEEE 2012, pp. 68-72.

[5] S. Kumar and S. Jena, "SCMRP: Secure cluster based multipath routing protocol for wireless sensor networks," in Proc. 6th Int. Conf. Wireless Commun. Sensor Netw., 2010 pp. 1–6.

[6] M. Radi, "LIEMR: A Low-interference energy-efficient multipath routing protocol for improving QoS in event-based wireless sensor networks," in Proc. Int. Conf. Sensor Technol. Appl., 2010, pp. 551–557.

[7] Choon-Sung Nam, Hee-Yeon Cho and Dong-Ryeol Shin, "Efficient path setup and recovery in wireless sensor networks by using the routing table," in Int.Conf. Educ. Technol. Comput., 2007, pp. 156–159.

[8] K Guan and L.-M. He, "A novel energy-efficient multi-path routing protocol for wireless sensor networks," in Proc.Int. Conf. Commun.Mobile Comput., Apr. 2010, pp. 214–218.

[9] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in Proc. Int. Conf. Netw. Protocols, 2001, pp. 14–22.

[10] Nils Aschenbruck, Jan Bauer, Jakob Bieling, Alexander Bothe, and Matthias Schwamborn, "A Security Architecture and Modular Intrusion Detection System for WSNs,"in Int. Conf.2012, pp.1-8.

[11] Rutvij H. Jhaveri, "MR-AODV: A Solution to Mitigate Blackhole and Gray hole Attacks in AODV Based MANETs," in 3rd Int. Conf. on Adv. Computing & Communication Tech.2012, pp.254-260.

[12] Sushmita Ruj, Amiya Nayak, and Ivan Stojmenovic, "Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications", in IEEE transactions on computers, vol. 62, no. 11, November 2013, pp 2224-2237.

[13] Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey," in proc IEEE Communications surveys & tutorials, vol. 15, no. 2, second quarter 2013,pp 551-586.

[14] Anri Kimura, Eitaro Kohno, and Yoshiaki Kakuda, "Security and Dependability Enhancement of Wireless Sensor Networks with Multipath Routing Utilizing the Connectedness of Joint Nodes," in 32nd Int. Conf. on Distributed Computing Systems Workshops 2012,pp 342-348.

[15] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari, Kumar Sidharth Choudhary, "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information," 4th Int. Conf. on Com. Sci. and Convergence Info. Tech., pp 824-828,2009.

[16] Moh. Wazid, A. Katal, R. Singh Sachan, R H Goudar and D P Singh, "Detection and Prevention Mechanism for blackhole Attack in Wireless Sensor Network", Int. Conf on Comm. and Signal Processing, April 3-5, 2013,pp 576-581, India.

[17] P. Chanak, I. Banerjee, H. Rahaman, "Distributed Multipath Fault Tolerance Routing Scheme for Wireless Sensor Networks", 3rd Int. Conf. on Adv. Comp. & Comm. Tech. 2012,pp 241-247.

[18] Madhu, Alpana Dahiya, Brahmprakash Dahiya, "Energy efficient data transfer in secure wireless sensor networks," 2nd Int. Conf. on Adv. Computing & Comm. Tech.2012,pp 495-499.

[19] Abhishek Jain, Kamal Kant, M. R. Tripathy, "Security Solutions for Wireless Sensor Networks", in 2nd International Conference on Advanced Computing & Communication Tech. IEEE 2012, pp 430-433.

[20] Zhang Yu, "The Scheme of Public Key Infrastructure for Improving Wireless Sensor Networks Security", in IEEE 2012, pp 527-530.

[21] Qian Yu and Chang N. Zhang, "A Secure Multicast Scheme for Wireless Sensor Networks", in 3rd FTRA Int. Conf. on Mobile, Ubiquitous, and Intelligent Computing ,IEEE 2012, pp.158-163.

