Volume 5, Issue 6, June 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/Sink Hole Attack Detection and Prevention in WSNs

Rakesh Kumar Gautam, Jay Prakash, Ajay Mishra, Sarvesh Kumar

Department of CSE , MMMUT Gorakhpur,

Uttar Pradesh, India

Abstract*— In a Wireless Sensor Network (WSN), Security is a major issue due to its dynamic topology, open wireless communication medium, lack of fixed infrastructure, intermittent connectivity, resource constrained sensor nodes. These weak entities make WSN easily compromised by an adversary to device abundant attacks resulting in disastrous consequences; Black Hole can be one of them. Wireless Sensor Networks (WSNs) are prone to various attacks. Black hole a kind of Denial of Service (DoS) attack is very difficult to detect and defend. In black hole attack, an intruder captures and re-programs a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. As a result any information that enters the black hole region is captured and not able to reach destination causing high end- to- end delay and low throughput. In this paper, we present some black hole detection and prevention methods researched by the active authors.

Keywords*— Black hole attack, DoS, Wireless Sensor networks, Sink hole attack, Network Security.

I. INTRODUCTION

Wireless sensor network (WSN) is a type of heterogeneous system that consists of thousands numbers of small; cost effective sensor nodes have some different features. Wireless sensor network (WSN) has low processing power and radio ranges, allowing very low energy consumption in the sensor nodes, and performing limited and specific sensing and monitoring functions [2 - 7]. Wireless sensor networks (WSNs) may create ad hoc networks that operate with little or no infrastructure and have attracted researchers for its development and many potential civilian and military applications such as environmental monitoring, battlefield surveillance, and homeland security. In many important military and commercial applications, it is difficult to secure a sensor network from malicious attacks. Wireless sensor network (WSN) needs a demand for providing security mechanisms in the network [1]. To design security protocols for Wireless sensor network (WSN) is a challenging work because of following factors:

- Wireless communication medium used in wireless sensor networks are accessible by everyone has a radio interface set at the same frequency. Because of this characteristic monitoring and taking part in communication process is convenient in wireless channel, and attackers can easily attacks into network.
- Sensor nodes have limited resources in the term of memory, computational capability. Due to this, effective security model is very critical to apply and implement because of complex nature of security model.
- Wireless sensor networks normally deployed in warlike region with ad-hoc architecture. Without any architecture it is very complex to continuous monitoring after network deployment. Because of this, attackers can easily attacks.

Security is one of the main challenges of any system and wireless sensor network may be influenced by different types of attacks. The security attacks concern for WSN because of physical accessibility of sensor and actuator devices in network and usage of minimal capacity in a network. These security holes causes attacks still present in WSN and can be handled using various security architectures and security services like integrity and authenticity, confidentiality in the wireless domain

In black hole attacks, a malicious node acts as a black hole [29] to attract all the traffic in the sensor network through a compromised node creating a metaphorical sinkhole with the adversary at the centre. A compromised node is placed at the centre, which looks attractive to surrounding nodes and lures nearly all the traffic destined for a base station from the sensor nodes. Thus, creating a metaphorical sinkhole with the adversary at the centre, from where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station.

The rest of this paper is organized as follows: Taxonomy of various threats and attacks in wireless sensor network has been given in section II. Security goals for sensor networks have been given in section III. Various black hole detection and prevention in wireless sensor network has been given in section IV. And finally conclusion is presented in section V.

II. TAXONOMY

In WSNs various types of threats and attacks may be possible because of it has no fixed infrastructure and strong security algorithms. Various type of threats shown in fig. 1.

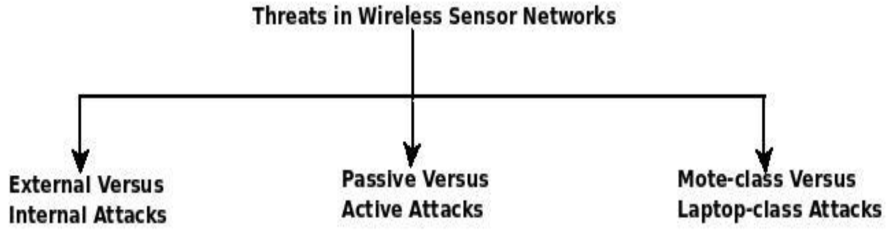
Threats in Wireless Sensor Networks
External Versus Internal Attacks
Passive Versus Active Attacks
Mote-class Versus Laptop-class Attacks

Fig. 1 depicts **t**axonomy of various threats in WSN

External versus internal attacks: In external type of attacks, attacker node belongs outside from WSN nodes. An external attacker has no access to most cryptographic materials in sensor network. In internal type of attacks, attackers belongs from the WSN nodes which are not performs its specified intended functions. Detection of Inside attacks are very difficult. Passive eavesdropping on data transmissions are resulting by external attacks and it can also pad extra unwanted data for the purpose of miss utilization of network resources and introduce Denial of Service (DoS) attack.

Passive versus active attacks: In passive attacks generally attackers are monitoring the packets that transmitted within a WSN. In active type of attacks generally attackers make some alteration in the data transmitted in WSN.

Mote-class versus laptop-class attacks: In mote-class (sensor-class) type attacks, a hostile attacks a WSN with the help of few nodes with same characteristics as that of network nodes. In laptop-class attacks, a hostile that uses more powerful devices like laptop, etc. and can do much more harm to a network than a malicious sensor node. These types of attackers can jam the radio link in its immediate vicinity. An attacker with laptop-class devices has greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna and hence they can affect much more than an attacker with only ordinary sensor nodes. A single laptop-class attacker might be able to eavesdrop on an entire network.

Different type of attacks may possible in wireless sensor networks that shown in following fig.2.

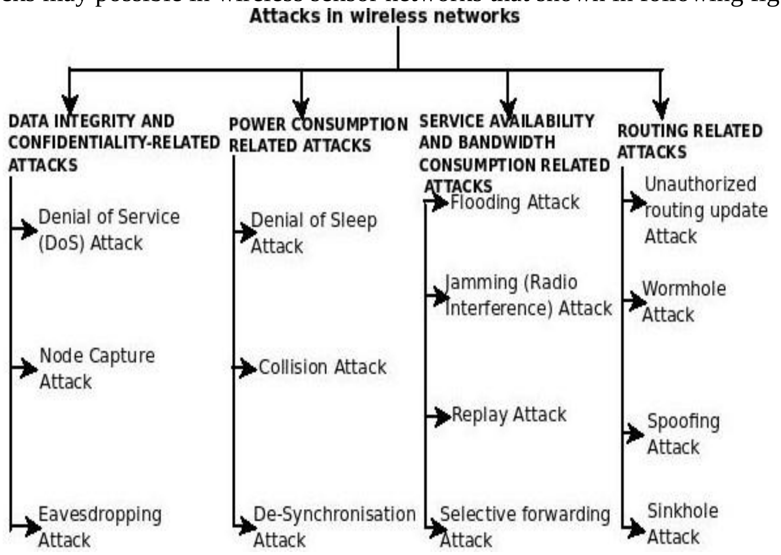
Attacks in wireless networks
DATA INTEGRITY AND CONFIDENTIALITY-RELATED ATTACKS
POWER CONSUMPTION RELATED ATTACKS
SERVICE AVAILABILITY AND BANDWIDTH CONSUMPTION RELATED ATTACKS
ROUTING RELATED ATTACKS
Denial of Service (DoS) Attack
Node Capture Attack
Eavesdropping Attack
Denial of Sleep Attack
Collision Attack
De-Synchronisation Attack
Flooding Attack
Jamming (Radio Interference) Attack
Replay Attack
Selective forwarding Attack
Unauthorized routing update Attack
Wormhole Attack
Spoofing Attack
Sinkhole Attack

Fig. 2 depicts taxonomy of various attacks in WSN

Data integrity and confidentiality-related attacks: In general, this type of attack attempts to reveal or compromise the integrity and confidentiality of data contained in the transmitted packets. Denial of services (DoS), Node Capture Attack, Eavesdropping Attack is the types of data integrity and confidentiality-related attacks.

Power consumption related attacks: One of the most valuable assets in wireless network is the power supply. In power consumption related attacks an attacker tries to exhaust the wireless device's power supply and it may degrade the lifetime of the network. A worst case scenario may even collapse the network communication. Denial of Sleep Attack, Collision Attack and De-synchronization Attack are power consumption related attack.

Service availability and bandwidth consumption related attacks: These attacks mainly aim to devastate the forwarding capability of forwarding nodes or consume meagerly available bandwidth; they are more likely related to availability of service and bandwidth consumption. These attacks can also be categorized as power consumption related attacks.

Routing related attacks: In general, these attacks attempt to change routing information, and to manipulate and benefit from such a change in various ways.

- Alteration in routing Information.
- An unprotected ad hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information.
- Form routing loops.
- Extend or shorten service routes.
- Generate false error messages.
- Increase latency.

III. SECURITY GOALS IN WIRELESS SENSOR NETWORKS

Main goal of security is to ensure safe and trusted transmission of data between nodes and base station in sensor networks. Researchers are developing different cryptographic approaches to achieve following goals for security [5].

- **Confidentiality:** Data confidentiality is ability to secure a message from third party like a passive attacker. That means communication between two sensor nodes should be confidential. This is most basic goal of network security. Confidentiality is an assurance of authorized access to information**.**
- **Authentication:** This ensures the receiver that data is coming from a trusted and claimed source and also for source that packet is going to a claimed destination.
- **Integrity:** Integrity in sensor network is ability to ensure that message during transmission is not modified or tempered. There may be a case that integrity of network be compromised even if confidentiality and authentication is ensured.
- **Non-repudiation:** This proves the source of a packet. In authentication the source proves its identity. Non-repudiation prevents the source from denying that it sent a packet.
- **Data Freshness:** Although if confidentiality and integrity of data is ensured, it is important to manage data freshness in network. This ensures that data sent is fresh and no old messages are resent again in transmission.

IV. DIFFERENT MECHANISM FOR DETECTION AND PREVENTION OF BLACK HOLE ATTACK

Virmani et al. (2014) proposed an exponential trust based mechanism to detect the malicious node. In this method a Streak counter was deployed to store the consecutive number of packets dropped and a trust factor was maintained for each node. The trust factor drops exponentially with each consecutive packet dropped which helps in detecting the malicious node. The method showed a drastic decrease in the number of packets dropped before the node being detected as a malicious node. [7]

Baviskar et al. The security in wireless sensor network is a main issue due to the limitations of power usage. Several techniques based on secret sharing and multi-path routing have been proposed in it However, these techniques are not very effective, and when demonstrate, they may even end up making black hole attacks more effective. Propose an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission and performance compare with multiple base stations and without multiple base station to prevent black hole attack. [8]

Wazid et al. proposed an algorithm used for detection and prevention of black hole attacks which is harmful for the wireless sensor networks. Black hole is just like as DOS attack. Black hole attacks degrading in the performance of network parameters are affected i.e end- to- end delay and throughput. [9]

Dighe et al. proposed a technique based on secret sharing and multipath routing to overcome black hole attacks in the network. However, these techniques were not very effective. The efficient technique that uses in multiple base stations deployed in the network to reduce the impact of black holes on data transmission. [10]

Wazid et al. proposed the comparative performance analysis of two WSN's topologies i.e. Tree and Mesh under black hole attack is done. If there is a WSN prone to black hole attack and requires time efficient network service for information exchange then Tree topology is to be chosen. If it requires throughput efficient and consistent service in the network then Mesh topology is used. An algorithm named as Topology Based Efficient Service Prediction (TBESP) algorithm was proposed depending upon the analysis done which will helped in choosing the best suited topology as per the network service requirement under black hole attack. [11]

Athmani et al. proposed the energy efficient intrusion detection system, to protect sensor networks from black hole attacks. The simple approach is based on control packets exchange between sensor node and the base station. [12]

Zhang et al. the location of each node in randomly deployed wireless sensor networks, and the detection of coverage holes. An improved hole detecting algorithm was proposed based on the Boolean sensing model .The algorithm used for hole boundary node by using diagram [13]

Amoli et al. studied the detection of the attack in very high speed networks by using the software network intrusion detection system .In this analyzing statistics of network flows increases feasibility of detecting intrusions within encrypted communications they had found the weaknesses and limitations of current unsupervised NIDS(Network Intrusion Detection System) [14]

Sheela .D et al. proposed a lightweight, fast, efficient and mobile agent technology based security solution against black attack for wireless sensor networks (WSNs). WSN has a dynamic topology, intermittent connectivity, and resource constrained device nodes. The scheme was used to defend against black hole attack using multiple base stations deployed in network by using mobile agents. The attack can be accomplished either selectively (e.g. by dropping packets for a particular network destination, a packet every n packets or every t seconds, or a randomly selected portion of the packets, which is called "Gray hole attack") or in bulk (by dropping all packets). Mobile agent is a program segment which is self-controlled. They navigate from node to node not only transmitting data but also doing computation. The benefit of using this mechanism is that it does not require more energy. [15]

Schaffer et al. reviewed the state-of-threat of clustering protocols in WSNs with special emphasis on security and reliability issue. They define taxonomy of security and reliability for cluster head election and clustering in WSNs. They propose a counter measures against typical attacks and show how they improve the discussed protocols. [16].

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained. Causal Productions has used its best efforts to ensure that the templates have the same appearance.

V. CONCLUSION

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. In this paper we summarized various black hole detection and prevention technique.

For the future work we will use the conclusion and suggestions given in this paper to propose security schemes reliable for detecting as well as preventing the wireless sensor networks.

REFERENCES

[1] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), vol. 02, pp570–580., 2012.

[2] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), vol. 2, no. 3, pp. 49-61, 2010.

[3] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Applications, Classifications, and Selections of Routing Protocols for Wireless Sensor Networks" International Journal of Advanced Engineering Sciences and Technologies (IJAEST), vol. 1, no. 2, pp. 85-95., 2010.

[4] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Routing Protocols in Wireless Sensor Networks – A Survey" International Journal of Computer Science and Engineering Survey (IJCSES), Vol. 1, no. 2, pp. 63-83., 2011.

[5] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Performance Evaluation and Comparison of Energy-efficient Routing Protocols for Wireless Sensor Network", Global Journal of Computer Application and Technology (GJCAT), vol. 1, no. 1, pp. 57-65., 2011.

[6] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy Efficient Transmission Error Recovery for Wireless Sensor Network", International Journal of Grid and Distributed Computing (IJGDC), vol. 3, no. 4, pp. 89-104., 2010.

[7] Dr. Deepali Virmani,, Manas Hemrajani and Shringarica Chandel., "Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network " Bhagwan Parshuram Institute of Technology,vol.1 Jan(2014).

[8] B.R. Baviskar and V.N.Patil "Black hole Attacks Prevention in Wireless SensorNetwork by Multiple Base Station Using of Efficient Data Encryption Algorithms" International Journal of Advent Research in Computer & Electronics, Vol.1, No.2, 2014.

[9] Mohammad Wazid , Avita Katal ,Roshan Singh Sachan , R.H Goudar and D.P Sing.,"Detection And Prevention Mechanism For Black hole Attack" in Wireless Sensor Network IEEE,(2013)

[10] Pranjali G Dighe , and Milind B Vaidya "Counter Effects of Black Hole Attack on Data Transmission in Wireless Sensor Network with Multiple Base Stations" International Journal of Engineering and Innovative Technology (IJEIT) Vol.3,Issue5, 2013.

[11] Mohammad Wazid, Avita Katal, Rooshsn Singh, Sachan , R.H Goudar and D.P Singh, "TBESP Algorithm for Wireless Sensor Network Under Black Hole Attack" IEEE International Conference on Communications (ICC) , 2013.

[12] Samir.Athmani., Djallei Eddine Boubiche and Azeddine Bilami ," Hierarchical Engery Efficient Intrusion Detection System For Black Hole Attacks in WSN" IEEE International Conference on Communications (ICC) , 2013.

[13] Yunzhou Zhang, Xiaohua Zhang, Zeyu.Wang and Honglei Liu.," Virtual Edge Based Coverage Hole Detection Algorithm in Wireless Sensor Network" IEEE International Conference on Communications (ICC), 2013.

[14] Payam vahdami Amoli , Timo Hamalainen , "A Real Time Unsupervised NIDS For Detecting Unknown And Encrypted Network Attacks in High Speed Network", IEEE International Conference on Communications (ICC), 2013.

[15] D.Sheela, V.R Srividhya, A.Begam, Anjali and G.M Chidanand," Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent" International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012)

[16] Peter.Schaffer, karoly.Farkas, Adam. Horvath Tamas Holczer and Levente. Buttyan, "Survey Secure and reliable clustering in wireless sensor networks: A critical survey", ACM, Computer Networks: The International Journal of Computer and Telecommunications Networking, (2012).