International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Detection of Sinkhole Attack in Wireless Sensor Network Using Ad-hoc on-demand Distance Vector

Hitesh Yadav[1] (Research Scholar)
Dept. of Computer Science & Engg.
Kalinga University, Naya Raipur
Chhattisgarh, India

Ms. Sana Tak[2] (Asst. Professor)
Dept. of Computer Science & Engg.
Kalinga University, Naya Raipur
Chhattisgarh, India

Abstract: **Wireless Sensor Network is a collection of the large number of small sensor node that has the capabilities to sense, collect, and disseminate information in many types of applications. This paper on exploring several types of security attack in wireless sensor network and counteragent against sinkhole attack. The Introduction sections give brief information about WSN, its components, and architecture. In next section discuss Sinkhole attack & its counteragent method and Then In Suggested Methodology Section author suggest a new technique to detect the sinkhole attack in a wireless sensor network (WSNs) which is based on the analysis of routing behaviour.**

Keywords: Wireless sensors networks (WSN), Security attacks in WSN, Sinkhole attack, Suggested methodology (AODV).

I. INTRODUCTION

Wireless sensor network is consisting of large number of small sensor nodes that has capabilities to sense, collect, and send to base station [9]. The sensor nodes are combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. Wireless sensor network consists of battery-operated sensor devices with processing unit and communicating components [1]. This paper is outlined as follows. Section I provide the introduction to WSN and covers the basic components and architecture of WSN. Section II describes various security threats of WSN. Section III describes the Sinkhole attack in WSN. Section IV describes some security counteragent mechanism against these security threats. Section V provides the conclusion of highlighted issues.

WSN ARCHITECHURE

WSN has the following network components sensor nodes, gateway, network manager and security manager.

A. Sensor nodes: - Each sensor node has following parts a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with other sensors and energy source like battery or embedded form energy generating system (solar panels).

B. Gateways: - Gateway is also known as Access point, it enables communication between host application and sensor nodes. A gateway is a network node that provides access to another network that uses different protocols and enables transmitted data to use its routing paths.

C. Network Manager: - A Network Manager is responsible for configuration of the network, scheduling communication between devices, management of the routing tables and monitoring and reporting the health of the network.

D. Security Manager: - The security manager is responsible for the generation storage and management of keys.

The base stations are one of most importance components of the WSN with more computational, energy and communication resource. They act as gateway between sensor nodes and the end user as they forward data from the WSN on to a server [1].

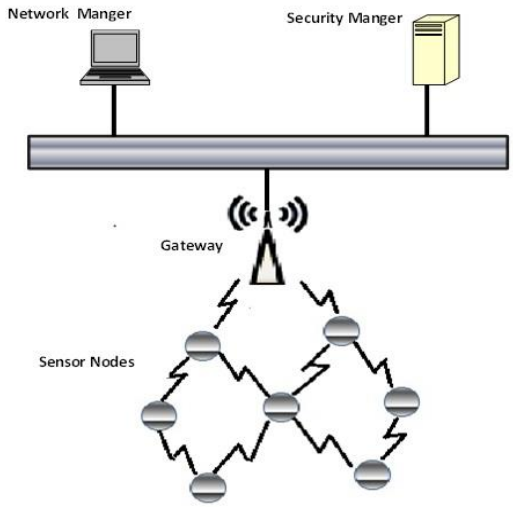

Figure 1: Architecture of a Wireless Sensor Network

II SECURITY THREATS

Wireless sensor network are vulnerable to security attacks due to the broadcast nature of the transmission medium. The attacks are basically classified into two categories i.e. passive and active attack.

1. Passive attack: The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. There are some common attacks against sensor privacy are:

❖ Monitor and Eavesdropping: It is most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

- Traffic analysis: Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activates can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network
- Camouflage Adversaries: One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

2. Active Attacks: The unauthorized attackers' monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

- Routing Attacks in Sensor Networks: The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the messages.
- Attacks on Information in transit: In a sense or network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished.
- Selective Forwarding: A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. In sensor networks, it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route.
- Sinkhole Attack: In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. In fact, this attack can affect even the nodes those are considerably far from the base stations. Figure c-1 shows the conceptual view of a sinkhole attack [1].

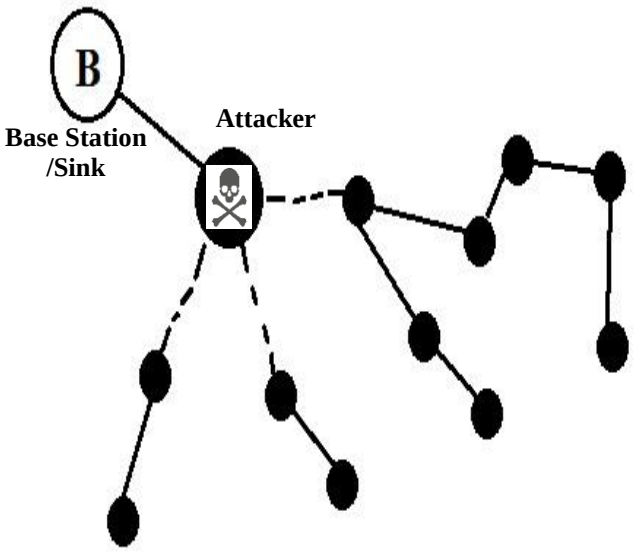

Figure 1: The Conceptual View of Sinkhole attack

- Wormholes Attacks: Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. Attackers here are strategically placed at different ends of a network. They can receive messages and replays them in different parts by means of a tunnel [3].

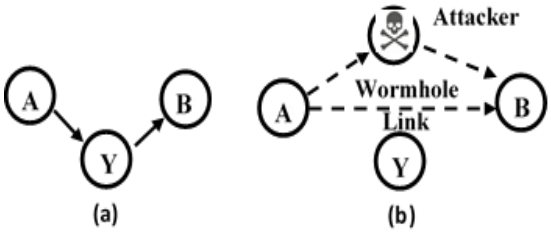

Figure 2 (a and b) shows a situation where a wormhole attack takes place.

When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multi-hop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole [2].

- HELLO flood attacks: An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN.
- Node Replication Attacks: Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted.
- False Node: A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur.
- Physical Attacks: Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

III SINKHOLE ATTACK

Sinkhole attack is an insider attack were an intruder compromise a node inside the network and launches an attack then that node try to attract all the traffic from neighbor nodes based on routing metric that used in routing protocol [18]. "Sinkhole attack" is one of the severe attacks in this type of network; this makes trustable nodes to malicious nodes that result in loss of secure information.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As an example, a laptop-class adversary has a strong power radio transmitter that allows it to provide a high-quality route by transmitting with enough power to reach a wide area of the network.

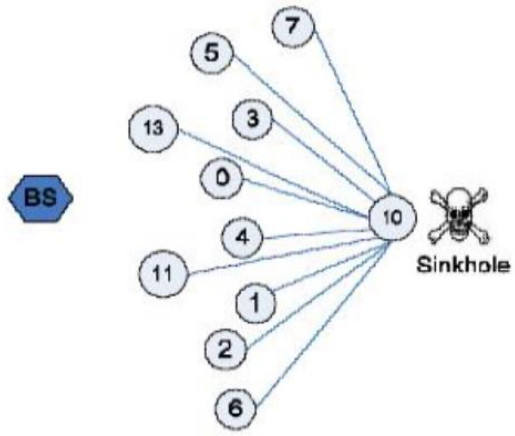

Figure 3: Demonstration of Sinkhole attack

Figure 4 denotes how sinkhole is created using wormhole. As shown in figure, one malicious node attracts all the traffic and make a tunnel with another malicious node to reach to the base station.

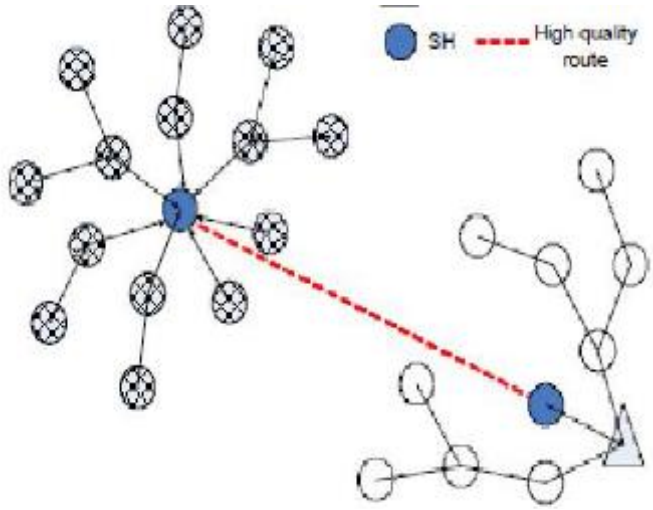

Figure 4: Sinkhole using wormhole attack [2]

IV COUNTERAGENTS APPROACH FOR SINKHOLE ATTACK

- Data Consistency & Network Flow Information Approach

  The approach presented involves the base station in the detection process, resulting in a high communication cost for the protocol. The base station floods the network with a request message containing the IDs of the affected nodes. The affected nodes reply to the base station with a message containing their IDs, ID of the next hop and the associated cost. The received information is then used from the base station to construct a network flow graph for identifying the sinkhole. The algorithm is also robust to deal with cooperative malicious nodes that attempt to hide the real intruder. The performance of the proposed algorithm has been examined through both numerical analysis and simulations. The results have demonstrated the effectiveness and accuracy of the algorithm [2]. They also suggest that its communication and computation overheads are reasonably low for wireless sensor networks.

- Hop Count Monitoring Scheme

  A novel intrusion detection system that detects the presence of a sinkhole attack is proposed in [5]. The scheme is based on hop count monitoring. Since the hop-count feature is easily obtained from routing tables, the ADS (Anomaly Detection System) is simple to implement with a small footprint. Moreover, the proposed ADS is applicable to any routing protocol that dynamically maintains a hop-count parameter as a measure of distance between source and destination nodes. The scheme can detect attacks with 96% accuracy and no false alarms using a single detection system in a simulated network.

- RSSI Based Scheme

  A new approach of robust and lightweight solution for detecting the sinkhole attack based on Received Signal Strength Indicator (RSSI) readings of messages is proposed in [2]. The proposed solution needs collaboration of some Extra Monitor (EM) nodes apart from the ordinary nodes. It uses values of RSSI from four EM nodes to determine the position of all sensor nodes where the Base Station (BS) is located at origin position (0, 0). This information is used as weight from the BS in order to detect Sinkhole attack. The simulation results show that the proposed mechanism is lightweight due to the monitor nodes were not loaded with any ordinary nodes or BS. The proposed mechanism does not cause the communication overhead.

- Mobile Agent Based Approach

  The scheme to defend against sinkhole attacks using mobile agents is proposed in [10]. Mobile agent is a program Segment which is self-controlling. They navigate from node to node not only transmitting data but also doing Computation. A routing algorithm with multiple constraints is proposed based on mobile agents. It uses mobile agents to collect information of all mobile sensor nodes to make every node aware of the entire network so that a valid node will not listen the cheating information from malicious or compromised node which leads to sinkhole attack. It does not need any encryption or decryption mechanism to detect the sinkhole attack. This mechanism does not require more energy than normal routing protocols.

- Rule Based

  The rules are designed based on the behavior or technique used to launch sinkhole attack. Then those rules are imbedding in intrusion detection system which runs on each sensor nodes. Those rules were then applied to the

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

packet transmitted through the network nodes. If any node violates the rules is considered as adversary and isolated from the network [9].

- Key management

  In this approach, the integrity and authenticity of packet travels within the network is protected by using encryption and decryption key mechanism. Any packet transmitted in the network is added with another message in a way that to access that message requires a key and any small modification of the message can be easily detected. Those keys also help nodes to check if the message comes from base station and check the authenticity of the message [12].

V SUGGESTED METHODOLOGY

This chapter suggested a new technique to detect the sinkhole attack in a wireless sensor network (WSNs) which is based on the analysis of routing behaviour. In the suggested methodology to detect the sinkhole attack in the wireless sensor networks the detection process is divided into three phase which are as follows:

Phase- I Topology Generation & Data transmission

Step 1: Invoke random topology generation.
Step 2: Invocation of route discovery phase.
Step 3: Data transmission.

Phase- II Sinkhole Implementation

Step 1: Source sends RREQ to the neighbourhood.
Step 2: If- neighbour node is an intruder it will send RREP with high sequence number and less hop count value.
Step 3: Else- neighbour node is destination, reply RP.EP to source.
Step 4: If- neighbour is not intruder and not destination, nod forward RREQ until it reaches to destination node or reaches end of the count node.
Step 5: On receiving various RREQ by malicious, it picks the reverse route path and forwards the forge RREQ with high sequence number & less hop count.
Step 6: On receiving forge RREQ by neighbour node, it believes sinknode is exist in the shortest path to send the data to destination node and starts forwarding the data to sinknode rather than genuine destination.

Phase- III Detection Phase

Step 1: Appointing highly connected node as a monitor node.
Step 2: Monitor node will keep track of routing RREQ and RREP
Step 3: Separating the forward route and reverse route from source to destination.
Step 4: If-node present in the reverse path but not in the forward path then assign node as a malicious or sinknode.
Step 5: Else-nodes present in both reverse and forward path, none of the intruder node.

VI CONCLUSION

In contrast to traditional networks, Wireless Sensor networks (WSN) are more vulnerable to attacks. As discussed, the sinkhole attack is one of the huge thread in a wireless that disturb the working of reactive routing protocol. This attack arises a big security issue as well as it increases a load on a particular area, increase energy consumption and network will goes down. Therefore, to deal with sinkhole attack number of techniques has been developed and each technique has their own pros and cons. The primary advantage of AODV reactive routing protocol is that source route does not needed to be enclosed within each packet. Means during packet transmission get easy and better than other routing protocol.

Among all major attacks on sensor networks, sinkhole attack is the most destructive routing attacks for these networks [2]. Majority of researches struggled with security challenges corresponding with availability of resources and mobility of wireless sensor nodes. Very few researchers managed to validate their security system using real wireless sensor network. Also, some of results showed low detection rate, high network overhead and high communication cost. Thinking like the attacker people understands better their goals and intentions. This will help them to protect their systems and networks better for the future intrusions; it will help us to create better intrusion detection systems and so on [11].

Even if there are so many types of attacks and the possibility of having the system compromised people must not give up to the security systems like firewalls, antivirus software, cryptographic systems and software Authors and Affiliations. [18].

ACKNOWLEDGMENT

. I would like to express my sincere gratitude to my guide “Ms Sana Tak” for giving me the opportunity to work on this topic. It would never be possible for me to take this project to this level without her relentless support and encouragement.

REFERENCES

[1] Vikash Kumar, Anshu Jain And P N Barwal (2014),” Wireless Sensor Networks: Security Issues, Challenges and Solutions”, International Journal of Information & Computation Technology (IJICT), Vol.04, No.8 (2014) pp.859868
[2] Vinay Soni,Pratik Modi and Vishvash Chaudhri (2013),” Detecting Sinkhole Attack in Wireless Sensor Network ”, International Journal of Application or Innovation in Engineering& Management (IJAIEM) Vol 2,Issue 2, Feb 2013.
[3] Dr. Shahriar Mohammadi,Hossein Jadidole slamy,“A Comparison of Physical Attacks On Wireless Sensor Networks” ,International Journal of Peer to Peer Networks(IJP2P) Vol.2, No.02,APR-2011
[4] G.Keerthana, G. Padmavathi (2016), “Detecting Sinkhole Attack in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique”, International Journal of Security and Its Applications (IJSIA),Vol. 10,No. 3 (2016).
[5] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao; “Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks” 15th IEEE ICN, 2007, ICON 2007, pp.176-181.
[6] Kesav Unnithan S L, Lakshmi Devi C, Sreekuttan Unnithan C (2015), “Survey of Detection of Sink Hole Attack in Wireless Sensor Netwok”, International Journal of Computer Science and Information Technologies (IJCSIT), Vol 6(6),2015,4904-4909.
[7] Md. Ibrahim Abdullah, “Detecting Sinkhole Attacks In Wireless Sensor Network using Hop Count”,IJCNS 2015,3,50-56
[8] Mohamed Lamine Messai, “Classification of Attacks in Wireless Sensor Networks”, ICT&A-APR-2014
[9] Maliheh Bahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat Heydari Yazdi and Sanaz Sadeghi (2012), International Journal of Computer Theory and Engineering (IJCTE), Vol. 4, No. 3 June 2012.
[10] George W. Kibirige,Camilus Sanga, “ A Survey on Detection of Sinkhole Attack in Wireless Sensor Network”,arXiv:1505.1941.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 05, May-2018

[11] D.Sheela, Naveen kumar. C & Dr. G.Mahadevan; "A Non Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, pp. 527-532
[12] Teodor-Grigore Lupu,"Main Types of attacks in Wireless Senors Networks",ISSN:1790-5109
[13] Papadimitriou, A., Fessant, L. F. and Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree-based routing in WSN. In Secure Network Protocols, NPSec 2009. 5th IEEE Workshop on (pp.43-48).
[14] Junaid Ahsenali Chaudhry,Usman Tariq,Mohammed Arif Amin,Robert G. Rittenhouse "Dealing with Sinkhole Attacks in Wireless Sensor Networks",AS&TL,Vol29(SecTech 2013),pp.7-12
[15] Chen, C., Song, M. and Hsieh, G. (2010). Intrusion Detection sinkhole attack in large scale wireless sensor network, In Wireless Communication, Networking and Information Security (WCNIS), 2010 IEEE International Conference on (pp. 711 -716). IEEE.
[16] Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu; "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" IEEE ICC, 2006, Volume 8, pp. 3383-3389.
[17] N.K. Sreelajaa, G.A. Vijayalakshmi Pai, "Swarm intelligence-based approach for sinkhole attack detection in wireless sensor networks", Elsevier Applied Soft Computing, Vol.19, (2014), pp. 68-79.
[18] Ms SanaTak, Hitesh Yadav,"A Surevy on Detecttion of Sinkhole Attack in Wireless Sensor Network",Vol.6, Issue 11.Nov-2017(IJERT).
[19] Rupinder singh,Dr.Jatinder Singh , "Attacks in WirelessSensor Networks:A Survey",IJCSMC, Vol. 5,Issue 5 May 2016,pg.10-16S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

AUTHOR PROFILE

Hitesh Yadav received the BE degree in Computer Science and Engineering from CSVT University, Bhilai Chhattisgarh and pursing M.Tech final year from Kalinga University Naya Raipur Chhattisgarh.

Ms. Sana Tak received the BE/B.Tech. and the M.Tech. Degree all from the Faculty of Computer Science and Engineering. She is an Asst. professor of Department of Computer Science and Engineering at the Kalinga University, Naya Raipur Chhattisgarh, India.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)