International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 11 | Nov 2020 www.irjet.net p-ISSN: 2395-0072

A Survey on various Detection Technique of Sinkhole Attack in WSN

Jay Pomal[1], Prof. Deepak Upadhyay[2]

[1]Dept. of Computer Engineering (Cyber Security), GTU – Graduate School of Engineering and Technology, Gujarat, India
[2]Dept. of Computer Engineering (Cyber Security), GTU – Graduate School of Engineering and Technology, Gujarat, India

---

Abstract – *The self-configuring type of network in which the sensor nodes are deployed in such a manner that they can join or leave the network when they want is known as wireless sensor network. The nodes start communicating with each other in order to transmit important information within the network. As this type of network is decentralized in nature, there are numerous malicious nodes which might enter the network. With the advancement of this technology, one of the major concerns these days is of security. The attacks are triggered within the network due to the presence of such kind of malicious nodes in the network which is of two parts active and passive types of attacks. Due to unique properties of wireless sensor network and many to one broadcasting nature various types of network layer attacks like wormhole, sinkhole, selective forwarding, sybil, hello flood, spoofed or altered information, etc. Among that sink hole attack is a type of attack in which malicious node attracts neighbor node by providing fake routing information that it has minimum distance from base station. A lot of work has been done in the area of detection of sink hole attack in WSN. In this paper we will study about sink hole attack in WSN and various techniques to identified over the years.*

Key Words: Wireless Sensor network, Sink hole attack, Network layer

1. INTRODUCTION

Wireless Sensor Networks are self-organizing, self-healing networks of small "nodes" and have huge potential across medical, smart city, disaster management, industrial, military and many other sectors.

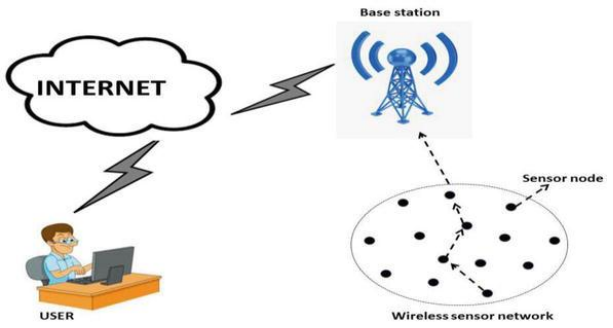

Figure 1 1: A typical wireless sensor network [14]

As wireless sensor networks are now essential part of nation's critical infrastructure like disaster management, critical military missions and training and health sector, security of wireless sensor network is must. Due to unique properties of wireless sensor network like limited battery power, limited memory storage, resource constrained and many to one broadcast nature is prone to various internal and external attacks. Many protocols have been introduced but most of them have not provided the desired security due to unique properties of WSN.

2. Protocol stack of WSN:

Before deep diving in research one should possess the knowledge functioning of wireless sensor network. Following is the architecture of wireless sensor network.

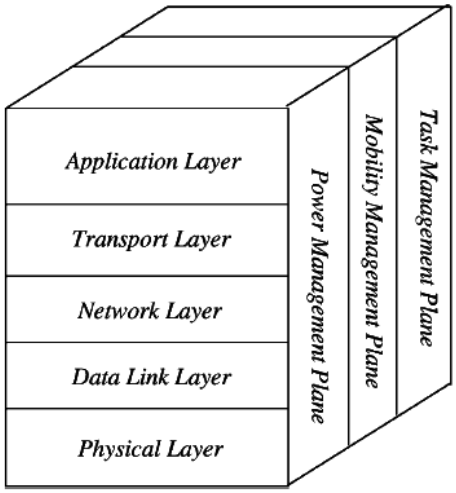

Figure 2 1: WSN Architecture

Unlike seven layers in OSI architecture, Wireless sensor network consists of 5 layers namely Application layer, Transport layer, Network layer, Data link layer or (mac layer) and physical layer with 3 cross layer plane Power management plane, Mobility management plane, Task management plane. Application layer provides different types of software usages according to task. Also makes hardware and software transparent to end users. Transport layer provides facility to maintain the flow of the data if required and this layer must require where system is planned to accessed through Internet or external networks. The main two task of network layers are data aggregation and data fusion. The essential part of network layer to route data provided by transport layer. Data link layer provides

functionality of multiplexing of data stream, frame detection and mac and error control. Physical layer task includes modulation, encryption, frequency selection and transmission and receiving techniques. In addition, the power, mobility, and task management planes monitor the power, movement, and task distribution among the sensor nodes. These planes help the sensor nodes coordinate the sensing task and lower the overall energy consumption.

3. Security Requirements for wireless sensor network

- Confidentiality
- Integrity
- Availability
- Authentication and authorization
- Non-Repudiation
- Freshness

3.1 Layer Wise attacks:

Table 1 : Attack in WSN

S. No	Layer	Attacks
1.	Physical	Jamming and Tampering
2.	Data Link	Collision Unfairness Exhaustion
3.	Network	Sinkhole Wormhole Sybil Selective Forwarding Hello Flood
4.	Transport	Flooding Desynchronization
5.	Application	Cloning Denial-of-service

3.2 Sinkhole Attack:

In a sinkhole attack intruder captures a legitimate node and update its routing information that it is one hop away or shortest distance from base station to attract all neighbor traffic.

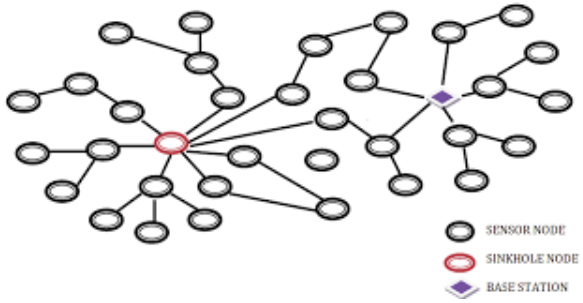

Figure 3.2 1: Sink hole attack

When intruder achieve this, it will launch a sinkhole attack. Sinkhole attack is an insider attack. Because of many to one communication nature of WSN where every node wants to send the information to base station, makes WSN vulnerable to sinkhole attack. Below we have presented an example of sinkhole attack in Mint-route protocol.

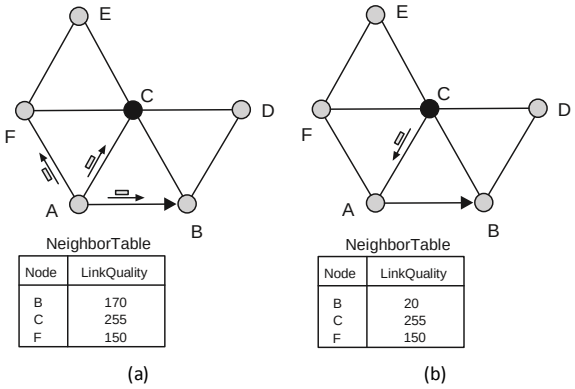

Figure 3.2 2: Example of sinkhole attack

Mint-Route protocol is a type of protocol which is commonly used in wireless sensor network. It was designed purposely for the wireless sensor network, it is light and suitable for sensor nodes which have minimum storage capacity, low computation power and limited power supply. Mint Route protocol uses link quality as a metric to choose the best route to send packet to the Base Station (Krontiris et al [10]). From above figure (a) when c launcher sinkhole figure, it will display its link quality with maximum value of 255. Still node A will not change its parent node to C from B. So as per figure (b) node C will send new route update packer that node B's link quality value falls up to 20 and node C will impersonate node B so that node A will believe that packet came from node B and node A will change its parent node from B to C.

Challenges in Detection of Sinkhole Attack:

1. Broadcast Nature of Communication (Many to one)
2. Attack is unpredictable
3. Insider Attack
4. Limited resources and Unique Properties
5. Physical Capturing

4. Literature Survey:

Prakash C Kala, Arun Prakash Agrawal, Rishi Rajan Sharma at [5] presented a novel technique to detect sinkhole attack. In that when throughput reduced than expected throughput, sensor node asks for the unique key of base station. Base station calculate key with Armstrong number. So malicious node which spoofs the identification of base station can not provide the unique key and detected as malicious node. Mohammad Wazid1, Ashok Kumar Das, Saru Kumari and Muhammad Khurram Khan at [6] proposed technique to identify sinkhole in hierarchical network using LEACH protocol. In that they proposed 2 algorithms in which they identify suspected node using sinkhole node existence algorithm and define suspected node type as SMD (sinkhole message modification node), SDP (sinkhole message dropping node) and SDL (sinkhole message delay node) by using sinkhole node identification algorithm. N. Mohammaed Yasin N. Balaji G. Sambasivam M. S. Saleem Basha P. Sujatha at [7] presented a hop count monitoring technique to identify sinkhole attack. This technique identifies attack with accuracy with 96% and applied to routing protocol that maintains dynamically a hop-count parameter. Arya I s and Dr. Bingu g s at [8] propose a cross layer approach for detection of sinkhole attack using mobile agent. The detection rate is increased as they identify affected cluster instead of affected node. Route was removed when it was accessed more frequently than expected to. For comparison they used re-clustering procedure with mobile agent procedure in terms of energy consumption and residual energy. Result proves mobile agent technique more efficient than re-clustering. Krontiris, I., Dimitriou, T., Giannetsos, T. and Mpasoukos, M. at [9] proposed a rule based technique to identify sinkhole attack. They presented 2 rules "for each overhead route update packet the ID of the sender must be different your node ID" and "for each overhead route update packet the ID of the sender must be one of the node ID in your neighbors". These 2 rules implemented in intrusion detection technique. When any node violates any of the rule than IDS will trigger an alarm but can not provide ID of the malicious node. Again Krontiris, I., Giannetsos, T. and Dimitriou, T. at [10] used same rule-based technique. In which they define 2 rules ""rule for each overhead route update packet the ID of the sender must be one of node ID in your neighbors" and "for each pair of parent and child node their link quality they advertise for the link between them, the difference cannot exceed 50." Roy, D.S., Singh, A.S. and Choudhury, S. at [11] proposed a dynamic trust-based technique in which every node calculates trust of their neighbor node based on experience of interaction and send the information to the base station. Then based on the trust information base station decides which node is sinkhole node. Thus, the trust value falls below normal value 0.5 for the node will be considered as sinkhole node. Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo, G. at [12] proposed a hybrid-based intrusion detection technique combining both anomaly-based and rule-based technique. In this hybrid intrusion detection was attached to every sensor node and shared their resources. The suspicious nodes put into black list and this information send to central agent for final decision. This technique was designed for static network. Sharmila, S., & Umamaheswari, G.at [13] proposed a technique using message digest algorithm to detect sinkhole attack. In that when an intruder node disguise itself to closest to base station by advertising fake routing information the sender node. Md. Ibrahim Abdullah, Mohammad Muntasir Rahman and Mukul Chandra Roy at [14] proposed a hop count-based technique in which at first base station first sends hello packets to construct neighbor database which contains nod_id of neighbor and hop count value. Node calculate average hop count value excluding lowest hop count value and nod_id. Then compares average hop distance with lowest hop distance if it is greater than threshold that mark it as suspicious.

Table 2 : Literature survey

Approach	Proposed Solution	Result
Rule Based. Krontiris et al 2008 [10]	They proposed detection rules that will keep aware legitimate node the existing of attack.	• They show how vulnerabilities of MultihopLQI can be exploited by sinkhole node and suggest the rules which make the protocol more resilient.
Anomaly based. Sharmila, S. et al 2011. [13]	They proposed message digest algorithm to detect sinkhole node.	• The results show the algorithm worked well when malicious nodes are below 50% • False positive rate was 20% (due to packet drop) that figure obtained when malicious node reach 50 • False negative error was 10% but was increasing

		when malicious node reach above 40
Anomaly based. N. Mohammaed Yasin et al 2017[]	A new hop count monitoring-based technique has been proposed to identify sinkhole attack.	• Result shows that proposed technique will detect sinkhole attack with accuracy of 94% ad will applicable to all routing protocol that maintains dynamic hop-counter parameter.
Key Management. Prakash C Kala et al 2020 [5]	A novel technique mutual authentication with use of Armstrong number has been produced to detect sinkhole attack.	• The proposed technique helps in reduction of energy consumption. • Result also shows minimum packet loss.
Hybrid base Coppolino et al 2007 [12]	They proposed intrusion detection system which was able to protect critical information from attacks directs from its WSN	• Detection rate was 95-97% when malicious node modified sensor packet. • Detection rate was 93-96% when malicious node modified the r • False positive rate is 3% • IDS usage in real sensor network was 734bytes (RAM) and 3208bytes (ROM)
Cluster based using Mobile Agent. ARYA I S et al 2017 [8]	A cross layered based mobile agent technique has been produced to detect sinkhole attack.	• Result shows that detection rate increased by identifying affected cluster instead of node. • Result also shows that mobile agent technique is more efficient than re-clustering in terms of energy consumption.
Hop count based. Md. Ibrahim Abdullah et al 2015 [14]	Proposed technique detects sinkhole attack by using hop count technique and this technique does not require any additional hardware nor the location of the node.	• Result shows that proposed technique detects sinkhole when it is located far from base station. • The result of detection is 100% within the transmission range of 10% to 60%. After that id decrease gradually with increase in transmission range.

5. CONCLUSION AND FUTURE WORK

In this paper we have first discussed about wireless sensor network and its architecture and security requirements for Wireless sensor network. We have also discussed about sinkhole attack and various technique to detect. This technique include namely anomaly based, rule based, hybrid based, hop-count based, cluster based and cryptographic based with various protocol like Mint-route, LEACH, ADOV and etc. We have identified that majority of techniques lack in term of security because of communication nature of wireless sensor network. Very few researchers were able to prove their technique using real wireless sensor network. Also, some technique showed low detection rate, high

communication cost and overhead. We have also analyzed that hierarchical WSN is better than flat based WSN for power and memory management. Future work should be direction of high detection rate, low network overhead, low communication cost and packet loss. Also, technique should be validated in real wireless sensor network. One can implement AI (artificial intelligence) to improve detection rate also LEACH protocol can be utilized to reduce power consumption.

REFERENCES

[1] Furrakh Shahzad, Maruf Pasha, Arslan Ahmad "A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures" International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 12, December 2016

[2] George W. Kibirige, Camilius Sanga "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 13, No. 5, May 2015

[3] S. Nithya, Dr.C. Gomathy "A Survey of Attacks in wireless Sensor Network" International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.26 (2015)

[4] S. Nithya, K.VijayaLakshmi , V.PadmaPriya "A Review of Network Layer Attacks and Countermeasures in WSN" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p- ISSN: 2278-8735.Volume 10, Issue 6, Ver. I (Nov - Dec .2015)

[5] Prakash C Kala, Arun Prakash Agrawal, Rishi Rajan Sharma "A Novel Approach for Isolation of Sinkhole Attack in Wireless Sensor networks" 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)

[6] Mohammad Wazid1, Ashok Kumar Das, Saru Kumari and Muhammad Khurram Khan "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks" SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2016; 9:4596–4614 Published online 17 October 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1652

[7] N. Mohammaed Yasin N. Balaji G. Sambasivam M. S. Saleem Basha P. Sujatha "ADSMS: ANOMALY DETECTION SCHEME FOR MITIGATING SINK HOLE ATTACK IN WIRELESS SENSOR NETWORK" International Conference on Technical Advancements in Computers and Communications 2017 IEEE

[8] ARYA I S, Dr. BINU G S "Cross Layer Approach for Detection and Prevention of Sinkhole Attack Using A Mobile Agent" Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017) IEEE Xplore Compliant

[9] Krontiris, I., Dimitriou,T., Giannetsos,T. and Mpasoukos, M. (2008). Intrusion Detection Sinkhole Attacks in Wireless Sensor Network. LNCS 4837, pp. 150-161

[10] Krontiris, I., Giannetsos, T. and Dimitriou, T. (2008). Launch Sinkhole Attack in Wireless Sensor Network; the Intruder Side.

[11] Roy, D.S., Singh, A.S. and Choudhury, S. (2008). Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management.

[12] Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo, G. (2010). An intrusion detection system for critical information infrastructures using WSN technologies.

[13] Sharmila, S., & Umamaheswari, G. "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms" 2011 International Conference on Process Automation, Control and Computing, IEEE

[14] Md. Ibrahim Abdullah, Mohammad Muntasir Rahman and Mukul Chandra Roy "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count" I.J. Computer Network and Information Security, 2015 MECS

[15] Imandi Raju and Pritee Parwekar "Detection of Sinkhole Attack in Wireless Sensor Network"

[16] Krontiris, I. Dimitrou, T. Freiling, F.C. (2007). Towards intrusion detection in wireless sensor networks. Proceedings of the 13th European Wireless Conference, Paris, France, April 2007.