A Survey On Sink Hole Attack in Wireless Sensor Networks

Venu H.D.[a],Chinnaswamy C.N.[b]

[a]PG Student,National Institue of Engineering,Mysuru,India
[b]Associate Professor,National Institute of Engineering,Mysuru,India

Abstract

Wireless Sensor Networks (WSN) are getting to be essential subject in research zone in view of its applications in critical regions like military, human services, savvy homes ,ecological observing and so forth., WSN is made out of a great many modest sensor nodes which are having the capacity of sensing, processing and communication. These sensors are having minimal effort on account of its low memory ,low calculation power, limited scope of correspondence capacity. In a large portion of the WSN applications, sensors are left unattended so security in these applications are vital in light of the fact that gate crasher may harm the sensor and get the critical information in order to do suspicious activities. One of the attack is Sink hole attack where foe or assailant tries to draw sensed data with the mean to counteract base station or sink node from accepting a total sensing information from nodes. Henceforth, attacker gets entire detected data from system and accomplish its objective. Along these lines, to overcome from this assault we need to track these sort of assaulted nodes in the system furthermore attempt to sidestep this in future. In this paper, we are doing Survey on various challenges in recognition of sink hole attack, diverse procedures for the discovery of sink hole attack and distinctive systems to sidestep this in future.

Keywords**:** *Wireless Sensor Networks(WSN), Base Station (BS),RSSI*

---

1. INTRODUCTION

Wireless Sensor network comprises of an arrangement of topographically dispersed sensor nodes, which constantly screen their environment and forward the detecting information to a base station through multi-hop routing. These systems utilize radio communication as a media for transmission which make them powerless to various sorts of attacks. We use the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. Sensor networks may consist of hundreds or thousands of low-power, low-cost nodes, possibly mobile but more likely at fixed locations, deployed en masse to monitor and affect the environment. Sensor networks often have one or more points of centralized control called base stations. A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it. In some previous work on sensor network routing protocols, base stations have also been referred to as sinks.

Base stations are typically many orders of magnitude more powerful than sensor nodes. They might have workstation or laptop class processors, memory and storage, AC power, and high bandwidth links for communication amongst themselves. However, sensors are constrained to use lower-power, lower bandwidth, shorter-range radios, and so it is envisioned that the sensor nodes would form a multi-hop wireless network to allow sensors to communicate to the nearest base station. A base station might request a steady stream of data, such as a sensor reading every second, from nodes able to satisfy a query. We refer to such a stream as a

data flow and to the nodes sending the data as sources.

It is clear that we must discard many preconceptions about network security: sensor networks differ from other distributed systems in important ways. The resource-starved nature of sensor networks poses great challenges for security.

- These devices have very little computational power: public-key cryptography is so expensive as to be unusable, and even fast symmetric-key ciphers must be used sparingly.

- With only 4KB of RAM, memory is a resource that must be husbanded carefully, so our security protocols cannot maintain much state.

- Also, communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800- 1000 instructions and as a consequence, any message expansion caused by security mechanisms comes at significant cost.

- Power is the scarcest resource of all: each milliamp consumed is one milliamp closer to death, and as a result, nearly every aspect of sensor networks must be designed with power in mind.

2. Security in Wireless Sensor networks

To provide security for WSN ,we will face many challenges and to achieve this security we must have some requirements.

2.1: Constraints in Wireless Sensor Networks:

A wireless sensor network consists of a large number of sensor nodes which are inherently resource-constrained. These nodes have limited processing capability, very low storage capacity, and constrained communication bandwidth. These limitations are due to limited energy and physical size of the sensor nodes. Due to these constraints, it is difficult to directly employ the conventional security mechanisms in WSNs. In order to optimize the conventional security algorithms for WSNs, it is necessary to be aware about the constraints of sensor nodes . Some of the major constraints of a WSN are listed below.

- Energy constraints : Energy is the biggest constraint for a WSN. In general, energy consumption in sensor nodes can be categorized in three parts: energy for the sensor transducer, energy for communication among sensor nodes, and energy for microprocessor computation. higher security levels in WSNs usually correspond to more energy consumption for cryptographic functions.

- Memory limitations: A sensor is a tiny device with only a small amount of memory and storage space. Memory is a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate results of computations. There is usually not enough space to run complicated algorithms after loading the OS and application code. The current security algorithms are therefore, infeasible in these sensors.

- Unreliable communication: Unreliable communication is another serious threat to sensor security. Normally the packet-based routing of sensor networks is based on connectionless protocols and thus

inherently unreliable. Packets may get damaged due to channel errors or may get dropped at highly congested nodes.

- Higher latency in communication: In a WSN, multi-hop routing, network congestion and processing in the intermediate nodes may lead to higher latency in packet transmission. This makes synchronization very difficult to achieve. The synchronization issues may sometimes be very critical in security as some security mechanisms may rely on critical event reports and cryptographic key distribution.

- Unattended operation of networks: In most cases, the nodes in a WSN are deployed in remote regions and are left unattended. The likelihood that a sensor encounters a physical attack in such an environment is therefore, very high. Remote management of a WSN makes it virtually impossible to detect physical tampering. This makes security in WSNs a particularly difficult task.

2.2 Security Requirements in WSNs:

A WSN is a special type of network. It shares some commonalities with a typical computer network, but also exhibits many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. The most important security requirements in WSN are listed below:

- Data confidentiality : The security mechanism should ensure that no message in the network is understood by anyone except intended recipient. In a WSN, the issue of confidentiality should address the following requirements. i) A sensor node should not allow its readings to be accessed by its neighbors unless they are authorized to do so. ii)key distribution mechanism should be extremely robust. iii)public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks.
- Data integrity: The mechanism should ensure that no message can be altered by an entity as it traverses from the sender to the recipient.
- Availability: This requirements ensures that the services of a WSN should be available always even in presence of an internal or external attacks such as a denial of service attack (DoS). Different approaches have been proposed by researchers to achieve this goal. While some mechanisms make use of additional communication among nodes, others propose use of a central access control system to ensure successful delivery of every message to its recipient.
- Data freshness: It implies that the data is recent and ensures that no adversary can replay old messages. This requirement is especially important when the WSN nodes use shared-keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN. A nonce or time-specific counter may be added to each packet to check the freshness of the packet.
- Self-organization : Each node in a WSN should be self-organizing and self-healing. This feature of a WSN also poses a great challenge to security. The dynamic nature of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station.

- Secure localization : In many situations, it becomes necessary to accurately and automatically locate each sensor node in a WSN. For example, a WSN designed to locate faults would require accurate locations of sensor nodes identifying the faults. A potential adversary can easily manipulate and provide false location information by reporting false signal strength, replaying messages etc.
- Time synchronization: Most of the applications in sensor networks require time synchronization. Any security mechanism for WSN should also be time-synchronized.

2.3 Attacks on different layers and countermeasures in Wireless Sensor Networks:

Table 1. shows layer wise attacks in WSN and possible countermeasures.

S.No.	Layer	Attacks	Counter measure
1	Physical Layer	• Jamming • Node Tampering • Eavesdropping	• Access Restriction • Encryption
2	Data Link Layer	• Traffic Manipulation • Identity Spoofing	• Misbehavior Detection • Identity Protection
3	Network Layer	• Sink hole attack • Sybil attack • Wormhole • Hello flood • Acknowledgment spoofing • Black Hole • False Routing • Packet Replication	• Fake messages • Routing Access Restriction • False Routing Information Detection • Wormhole Detection
4	Transport Layer	• Flooding • De-synchronization	• Limiting Connection Numbers • Authentication
5	Application Layer	• Malicious Code Attacks • Repudiation Attacks • Clock Skewing • Selective Message Forwarding • Data Aggregation Distortion	• Data Integrity Protection • Data Confidentiality Protection

Table 1 : Layer wise attacks in Wireless Sensor networks(WSN)

3. Sink Hole attack

Sinkhole attack is considered as one of the serious assaults that is propelled by a compromised node to occupy the system activity far from the intended activity, Through this system sinkhole node endeavors to attract all system movement to itself. From that point it modifies the data packets or drops the packets noiselessly and finally decimate the system. A sinkhole assault causes a genuine risk to sensor systems.

Sinkhole assaults (see Fig. 1) commonly work by making a malicious node look particularly attractive to neighbor nodes regarding the routing algorithm. Due to either the genuine or envisioned good quality route through the malicious node, it is likely each neighboring node of the foe will forward data packets for a sink through the foe, furthermore propagates the engaging quality of the route to its neighbors. Viably, the enemy makes a extensive "effective reach", pulling in all traffics bound for a sink from hubs a few hops far from the malicious node. So all the sensed data are collected by malicious node which is under the control of attacker. He may alter or drop the data packet and may destroy the whole network.

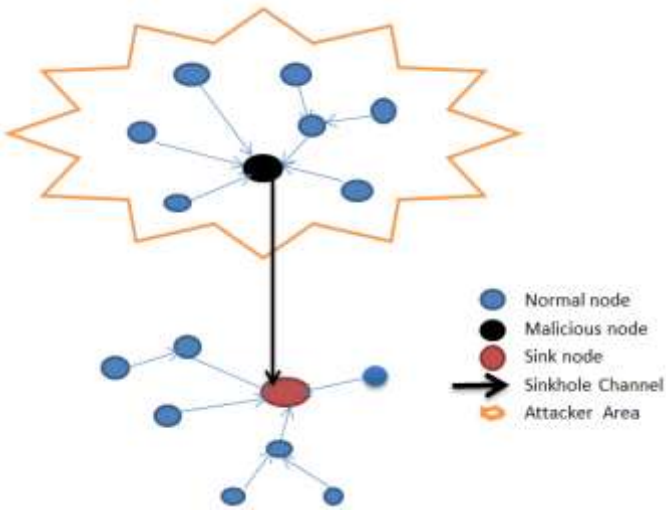

Fig. 1: Sink Hole Attack

The base station is kept by the sinkhole attack from accomplishing complete and precise sensing data, and hence it is brought about a vital risk which is basic for wireless sensor systems. Actually, this happens due to the unprotected remote connections, the organization of the sensors in open territories, what's more, the frail calculation and battery control.

4. Challenges in Detection Of Sink hole Attack

- Asset Constraints
- Physical assault
- Sinkhole attack is uncertain
- Insider Attack
- Correspondence Pattern in WSN

4.1 Asset Constraints

The restricted power supply, low correspondence extend, low memory limit and low computational power are the fundamental compelled in Wireless Sensor network that thwart usage of solid security system. For instance the solid cryptographic strategy that utilized in other system can't be actualized in this system because of low computational power and low memory limit. In this manner less solid key are considered which is good with available assets.

4.2 Physical assault

A Wireless sensor nodes ordinarily conveyed in antagonistic environment and left unattended. This gives a open door for an interloper to assault a hub physically what's more, access all important data.

4.3 Sinkhole attack is uncertain

In wireless sensor network the data are transmitted based on routing metric utilized by various routing protocols. The bargained hub utilized its routing metric that utilized by routing protocol to mislead his neighbours with a specific end goal to dispatch sinkhole assault. At that point every one of the information from his neighbours to base station will go through malicious node. For instance the methods utilized by malicious node as a part of system that utilized TinyAODV convention is distinctive to the one utilized another convention like MintRoute convention. In MintRoute they utilized connection quality as course metric while in TinyAODV they utilized number of hops to base station as routing metric. In this manner the sinkhole assault strategies is changed in view of routing metric of different routing protocols.

4.4 Insider Attack

Insider assault and outcast assault are two classes of assault in remote sensor organize. Outside assault is when attacker is not a portion of system. In inside assault the attacker bargains one of the true node through node hardening or through shortcoming in its framework programming then malicious node infuse false data in system after listen to sensed data. Inside assault can upset the system by altering routing packet. Through malicious node sinkhole attack draw in almost all the activity from specific territory in the wake of making that malicious node alluring to neighbor nodes .

The truth of the matter is that malicious node has satisfactory get to benefit in the system and has learning relating to profitable data about the system topology this made difficulties in recognizing. Base to that circumstance even cryptographic can't guard against insider assault in spite of the fact that it gives honesty, secrecy and validation. Therefore the interior assault has more genuine effect on victim system contrasted with outside assault.

4.5 Correspondence Pattern in WSN

Every one of the messages from sensor nodes in wireless sensor system are bound to base station. This made open door for sinkhole to dispatch an assault. Sinkhole assaults regularly happen when malicious node send fake routing data to different nodes in the system with point of pulling all network traffic as could be expected under the circumstances. In view of that correspondence design the interloper which target the node which are near to base station as opposed to focusing on all nodes in the system. This is considered as difficulties in light of the fact that the communication design itself gives chance to assault.

5. Approaches for the Detection Of Sink hole Attack

a)Control field monitoring:

The proposed calculation in [1]works by looking at the control fields of the received data packets with the first control packet, at whatever point a node needs to send information to the BS, it first sends a control packet straightforwardly to the principle BS. At that point it starts to send information packet in type

of hop to hop directing to the BS. After the information packet touches base at the BS, it thinks about the control fields of the got information packet with the first control packet. On the off chance that any controls have been identified to these control fields or misfortune in the information packet, the BS identifies that there is a noxious node in that way by utilizing the proposed technique.

b) Hop Count monitoring:

Proposed algorithm in [2] shows hop count monitoring scheme for detection of sink hole attack in wireless sensor networks. Since the link count feature is effectively get from routing tables, the ADS (Anomaly Detection System) is easy to implement with a simple impression. Additionally, the proposed ADS is pertinent to any routing protocol that progressively keeps up a link count parameter as a measure of separation amongst source and destination.

c) RSSI based scheme:

Another approach [3] of vigorous and lightweight answer for recognizing the sinkhole assault in light of Receive d Signal Strength Indicator (RSSI) readings of
messages is proposed. The proposed arrangement needs cooperation of some Extra Monitor (EM) nodes separated from the customary nodes. It utilizes estimations of RSSI from four EM nodes to decide the position of all sensor hubs where the Base Station (BS) is situated at source position (0, 0). This data is utilized as weight from the BS with a specific end goal to distinguish Sinkhole assault.

d) Monitoring node's CPU usage:

The CPU use of every sensor node is observed furthermore [4], breaks down the consistency of the CPU utilization. By checking the CPU utilization of every node in altered time interim, the base station figures the distinction of CPU use of every node. Subsequent to contrasting the distinction with a threshold, the base station would distinguish whether a node is pernicious or not.

e) mobile-agent based approach

Mobile agent [5] is a program section which is self-controlling. They explore from node to node transmitting information as well as doing calculation. A routing calculation with various requirements is proposed in view of portable specialists. It utilizes mobile agents to gather data of all versatile sensor nodes to make each node mindful of the whole system so that a legitimate node won't listen the fake data from malicious node which prompts to sinkhole assault. It needn't bother with any encryption or decoding component to distinguish the sinkhole assault. This system does not require more vitality than ordinary routing conventions.

f) Using Message Digest Algorithm

The primary objective of the convention [6] is to identify the correct sink hole utilizing the one way hash chains. In the proposed strategy destination recognizes the assault just when the digest got from the trustable forward way and the digest got through the trustable node to the destination are distinctive. It additionally guarantees the information trustworthiness of the messages exchanged utilizing the trustable way.

6. Approach to mitigate Sink hole attack in WSN

a)RESIST-1 AND RESIST-0 PROTOCOLS

These are [7] Resilient and Simple Topology-based reconfiguration conventions. RESIST-1 keeps a noxious node from adjusting its promoted distance to the sink by more than one hop, while RESIST-0 does

not permit such lying at the cost of extra multifaceted nature.

RESIST-1: The reconfiguration begins by the sink sending a Hello(epoch, tokens) message to every one of its neighbors, where epoch is an entirely expanding timestamp, picked by the sink and tokens is a rundown of tokens [T0, T1, T2, ..., TR]. Where each token is (k, epoch) and k is token number.
At the point when a sensor gets a Hello message, and subsequent to checking that the tokens are effectively marked by the sink .it does the following. On the off chance that the epoch is new, it recollects the character of the node sending it (i.e., his parent), and engenders the Hello message in the wake of evacuating the littlest token from the list of tokens. In the event that the epoch is as of now known,yet the Hello message
publicizes a shorter hop separation to the sink (i.e., contains a littler token), the node may take after various approaches. A Selfish approach would just overhaul the hub itself, while a gossip approach would likewise proliferate another Hello message to the neighbors.

Every sensor recalls as its parent, from which it got
the littlest token marked by the sink for the latest epoch. Take note of that the token number of the littlest token is additionally the hop distance to the sink. On the other hand, sensors can likewise keep in mind every one of the nodes that publicize the most shortest distance for a given epoch.

RESIST-0: To provide higher resilience, it is the newly proposed complex reconfiguration protocol (RESIST-0). This protocol is inspired by a protocol used to measure availability in peer-to-peer networks , where recently produced sets of cryptographic keys are diffused in the system at each round. The sink sends a Hello(epoch, [T0, T1, ..., TR]) message. The reconfiguration convention is the same as RESIST-1, with the exception of that, at the gathering of another epoch and before picking a sensor N as its parent, a sensor M challenges the sensor N first by sending a Challenge(k, epoch) message. Essentially, this message requests that N demonstrate its distance k from the sink (i.e. that it has a duplicate of the token Tk). Sensor Y answers with a message ChallengeReply Which is scrambled by private key of token.

Since a sensor can sign the second part of the ChallengeReply message, if and just if it knows the private key for the token k, it is incomprehensible for a malicious sensor (without agreement) to effectively answer to a Challenge. Besides, malicious node can't indeed, even do the assault that we portrayed for RESIST- 1. Basically, not dropping the littlest token would come up short, since they would not have the capacity to react to the Challenge for the shorter hop count tally. Subsequently, RESIST-0 gives solid flexibility against sinkhole assaults

b) By hiding the location of Sink:

For sensor networks deployed to collect and transmit events into a sink node, sink anonymity is a critical security property. If the mislead or cheat the location of sink from attacker , we may achieve the mitigation of sink hole attack.so preserving location of sink is very important.

Some of the techniques for preserving location of sink are broadcast fake messages along with real data so that attacker can’t get real sink since uniform flow of traffic in the network. Another approach is use of fake sinks approach along with real sink. Attacker is confused of which one is real sink and which one is fake sink. One more is using Clustering or Zone routing protocol we can detect and mitigate the sink whole attack in wireless Sensor networks.

7. CONCLUSION

In this paper, we have scrutinized sink hole attack properties, their behavior. Challenges in detection of sink hole attack like Asset Constraints, Physical assault, Sinkhole attack is uncertain, Insider Attack, Correspondence Pattern in WSN ,various approaches for the detection of sink hole attack like Control field monitoring, RSSI based scheme, Monitoring node's CPU usage, mobile-agent based approach, Using Message Digest Algorithm, Hop Count monitoring and approaches to mitigate sink hole attack like RESIST-1 and RESIST-0 protocols and preserving location of sink from intruder.

8. REFERENCES

[1]Maliheh Bahekmat, et al, "A novel algorithm for detecting Sinhole attacks in WSNs", International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012, pp 418-421.

[2]Daniel Dallas, Christopher Leckie, Kotagiri amamohanarao; "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks" 15th IEEE International Conference on Networks, 2007, ICON 2007, pp.176-181.

[3]Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth; "Detecting Sinkhole Attacks in Wireless Sensor Networks" ICROS -SICE International Joint Conference 2009, pp. 1966 -1971.

[4]Changlong Chen, Min Song, and George Hsieh; "Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks" IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010, pp. 711-716.

[5] D.Sheela, Naveen kumar. C and 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

[6] S.Sharmila and Dr G Umamaheswari; "Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms" International Conference on Process Automation, Control and Computing (PACC) 2011, pp. 1-6

[7] Anthonis Papadimitriou; Fabrice Le Fessant; Aline Carneiro Viana; Cigdem Sengul; "Cryptographic protocols to fight sinkhole attacks on tree-based routing in Wireless Sensor Networks" Secure network Protocols, 2009 NPSec 2009.5th IEEE workshop