ISSN 2319 - 6629
Volume 10, No.4, June - July 2021
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt01102021.pdf
https://doi.org/10.30534/ijwcnt/2021/011042021

Survey on Approaches to Detect Sinkhole Attacks in Wireless Sensor Networks

Madhu Nagaraj[1], Rampur Srinath[2]
[1]Mtech Student, Dept of IS&E, NIE, Mysore, India, madhunagaraj.2007@gmail.com
[2]Associate Professor, Dept of IS&E, NIE, Mysore, India, rampursrinath@nie.ac.in

ABSTRACT

Due to the wide range of applications in public and military domains, wireless sensor network (WSN) is evolving as a popular technology. This WSN consists of a large number of sensors that are spread across a geographical area that are self-configuring in nature. These nodes are of low cost and resource-constrained nodes. Because these reasons the network becomes vulnerable to many network attacks. There are many types of attacks among which one of the serious attacks is the sinkhole attack, which is one of the destructive routing attacks. It causes the adversary node to attract all or most of the traffic from the neighbors by broadcasting false routing updates of having the shortest path to the central station. This paper is a survey on various methods implemented to overcome sinkhole attacks like Hop Count Monitoring scheme, Key Management Approach, Message-Digest Algorithm.

Key words: Hop Count Monitoring Scheme, Message-Digest Algorithm, Sinkhole attack, Wireless Sensor Network.

1. INTRODUCTION

A wireless sensor network (WSN) contains a collection of tiny sensor nodes that are autonomous and can communicate with each other using a wireless radio device. These nodes have the ability to sense the surrounding environment like temperature, humidity, and illumination and send these sensed data to the central station. Mainly the communication happens through many hop patterns after which each source node sends the data to the central station, where these sensor nodes have less energy, computations, and communication links. This has major applications in various fields like medical science, inventory tracking, military surveillance, environment monitoring, and seismic detection, etc. Figure 1 shows the WSN structure. Wireless Sensor Network Security is one of the most challenging issues in WSN. Here we are mainly focused on routing attack in wireless sensor network, the sinkhole attack. In the routing attack the main aim is to modify the routing protocol so that all the traffic is lured by the adversary node. The sinkhole attack through a compromised node attracts all traffic by broadcasting false information to the neighbor nodes that it has the shortest route to the destination and thus disturbs the network topology. The attack can be reduced by the compromised node by using various parameters and thus we can reduce the attack in WSN. In this paper we have studied sinkhole attacks in WSN and analyzed various sinkhole detection and mitigation methodologies. The rest of the paper is divided as follows: Sinkhole attack is explained in section 2. Section 3 explains the challenges in the detection of sinkhole attacks in WSN. Section 4 explains some of the various approaches proposed by different researchers for detecting the sinkhole attacks, followed by a conclusion in section 5.

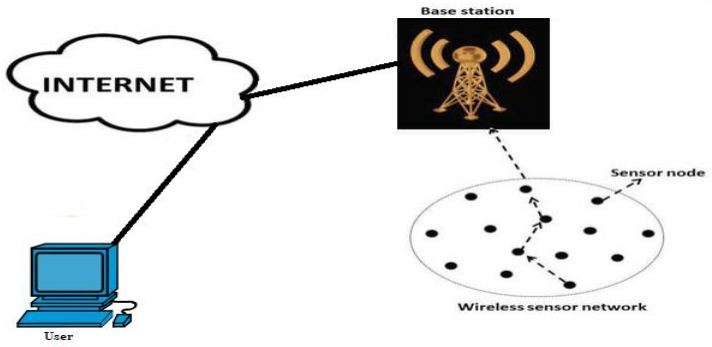

Figure 1: Wireless Sensor Network

2. SINKHOLE ATTACK

A sinkhole attack is a type of network layer attack in the wireless sensor networks where the malicious node tries to allure the network traffic by alleging a false routing update as it has the shortest path to the base station. Because of these updates, the packets get pulled towards the malicious node. After the adversary gets succeeded in achieving to convince the neighbor nodes that it has the shortest path, it launches an attack. During this attack the malicious node starts dropping the packets, thus blocking the correct packets from reaching the central station. And finally on dropping some important packets may completely disorganize the sensor network. Figure 2 shows the illustration of sinkhole attack.
This sinkhole attack may disturb the security measures in almost every layer of the protocol stack. The communication

pattern within the wireless sensor network is many to one communication where each node sends data to the base station, makes it susceptible to sinkhole attack. Based on this communication flow the sinkhole attack does not require to target all nodes in the network but mainly targets the ones which are near to the base station.

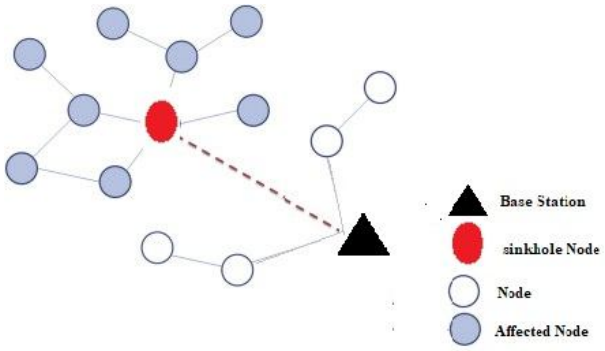

Figure 2: Sinkhole Attack

3. CHALLENGES IN DETECTING SINKHOLE ATTACK

The following section is a list of challenges that have been identified in the detection of sinkhole attacks in the network.

A. Communication Patterns – In the wireless sensor network, every message from the sensor nodes are meant to the central station. This situation provides an opportunity to launch a sinkhole attack. The main aim of the malicious node in the sinkhole attack is to attract all the traffic in the network towards itself by sending false routing updates to all other nodes in the network. The intruder node will target only the nodes which are closer to the base station instead of all the nodes in the network based on the communication pattern. As the communication pattern itself provides a chance for an attack, it is considered a big challenge.

B. Unpredictability of sinkhole Attack – The transmission of the packets in the wireless sensor network is mainly based on the routing metrics. The malicious node uses its routing metric by providing fake routing updates to its neighbors for launching the sinkhole attack which makes all the data from its neighbors to the central station is passed through the malicious node. For example, the Tiny AODV protocol uses a technique that is different from that used by the Mint Route protocol to launch a sinkhole attack. The Tiny AODV uses the number of hops to the central station as the routing metric whereas the Mint Route protocol uses the link quality as the routing metric. Hence the sinkhole attack remains unpredictable to be detected with common technique in all the networks.

C. Insider Attack – In the wireless sensor network, there are two categories of attack namely insider attack and outsider attack. In the outsider attack, the intruder is not a part of the network. In an insider attack, the attacker or intruder concedes one of the legitimate nodes of the network to become a malicious node by node tampering or through any of the system software weakness of the node. As the compromised node has listened to all required info, it injects false routing information in the network. Thus the insider attack disrupts the network by routing modification. By sinkhole attack, the malicious node attracts all the traffic towards itself. As the malicious node has appropriate access privileges in the network and has all information about the network topology as well, it becomes challenging in detecting it. In this situation, the cryptographic technique also cannot defend against insider attack even though it provides confidentiality, authenticity, and integrity. Hence insider attack leaves a major impact.

D. Resources Constraints Limits Detection – The resource constraints in wireless sensor networks like low computational power, low memory capacity, low communication range, and limited power supply disrupt the implementation of a strong security mechanism. Because of this low computational power and low memory capacity, the cryptographic methods which is a strong security method used in other networks cannot be implemented in WSN. Therefore little weaker security mechanisms are adapted that is compatible with available resources and thus provides an opportunity to launch an attack.

E. Physical Attack Vulnerability – The sensor nodes in the WSN are sometimes deployed in an unfriendly environment and many times it remains unattended. This gives a scope for the attacker to physically attack and get all necessary information related to the communication pattern and the network structure.

4. RELATED WORK

Different approaches have been suggested by various researchers for detecting sinkhole attack in WSN.

Message Digest Algorithm – A message-digest algorithm using cryptography is proposed by Sharmila and Umamaheswari [9], to detect the sinkhole attack in WSN. It uses an anomaly detection scheme mainly focused on detecting sinkhole with a high detection rate. It uses SHA-1 and MD5 hash functions. In this method whenever the node advertises the message, the digest of the message is found using the union of SHA-1 and MD5 algorithm. All the nodes in the network will have the address or the position of the node which is the nearest node in the path to the base station. When the new path info is advertised to provide a short path to the base station, then other nodes create a digest of the message and send it via the original path and the advertised path, where both paths meet at any node or the base station. If the new node is the intruder, then the data will be modified, which in turn modifies the message digest of the data. Thus when the two messages are checked at the point of

intersection, if there is a mismatch in the message digests it can be found whether the node is trustable or malicious.

RSSI Based Scheme – A scheme based on received signal strength indicator (RSSI) is proposed by Tumrongwittayapak and Varakulsiripunth [10] for detecting sinkhole attack. This scheme initially requires four extra monitor (EM) nodes to decide the position of all sensor nodes in the network. Based on the current info a visual graphic of the exploratory network is created by the EM nodes. These EM nodes have a high range of communication. Whenever a sensor sends messages to all other nodes in the network, these four EM nodes receive the message and the RSSI values. Based on the RSSI value, they calculate the position of the sender and send it to the central station with source ID and next hop, and also the visual graphic map (VGM) is updated. This process is done as soon as the nodes are deployed. If the normal flows in the visual graphic map and the flows of received messages do not match then there is a possibility of a malicious node present between the source and destination node on the visual graphic map. For detecting the sinkhole nodes all the messages are finally sent to the central station. The adversary node is then detected and detached from the network by the central station by using the VGM value.

Based on Hop Count Monitoring – A scheme based on hop count monitoring for detecting sinkhole attacks in wireless sensor networks is proposed by Abdullah et al. [1]. In this paper, they have presented a new algorithm that is easy and effective to detect and locate sinkhole attacks in wireless sensor networks. This technique does not require additional hardware, node location, or send any info to the base station. The common technique for all routing protocols is the distance of each node from the central station. When a sinkhole node publishes its shortest hop distance from the central station, the neighbors of this node compares the lowest hop distance with the hop distance database. The database is created in the network initialization phase. If it is remarkably low then we can conclude that there may be a chance of sinkhole attack [3]. The sinkhole node detection rate is increased when the distance of the nodes is increased from the base station. The detection rate is 100% when a node locates at a 70- meter distance from the base station for a minimum three-hop difference.

Artificial Bee Colony Based Method – A new method to detect and mitigate sinkhole attacks is proposed by Nithiyanandam et al [8]. The proposed method uses an Artificial Bee Colony (ABC) algorithm to detect and remove the sinkhole nodes. All the sensor nodes in the wireless sensor networks look on to the received packets on the route update request and the sinkhole node is detected based on the rule matching method by using the ABC algorithm. A novel approach called artificial bee colony attack detection (ABC-AD) is used here to detect sinkhole attacks in WSN. In this approach the bees in the network choose some node randomly stating that it can probably be the sinkhole node, this node will be compared with the node ID of the node sending the route update packet. If the chosen node is a malicious node then the energy value is assigned to '0'. If at all the selected node ID is greater than the node sending the route update packet, then the energy value will be '1' and for each node incremented with +1 till sinkhole node is found. If the selected node ID is less, then the energy value is '-1'and decremented for each node till the sinkhole node is detected. Upon receiving each node will compare the request with the rule set, which contains neighboring nodes of each sensor node and its respective link quality. If at all there is a match, the route will be updated. And if there is any mismatch, then it indicates the presence of a sinkhole attack. If there is a mismatch in node id's then it is concluded that the route update packet is from the malicious node. And if a mismatch occurs in link quality then it means the node is impersonating other nodes. The algorithm is used to detect the sinkhole node formed on the rule matching method which has less computational time.

Using HEED Clustering Concept – A sinkhole attack detection and prevention using the clustering protocol is proposed by Vishwas et al. [11]. In this approach cluster heads are used instead of mobile agents for the broadcasting messages. Here networks are initially divided into clusters with a cluster head in each cluster which is directly connected to the base station. The high energy node is selected as a cluster head in each round. The cluster head randomly selects a set of nodes and to these selected nodes a unique value is broadcasted to their authentication keys. The slice method is used when any node is sending the data to other nodes in the group. Slices of data are sent by encrypting it with individual authentication keys. At the receiving end, it is decrypted, summed up, and sent to the cluster head, which later aggregates and encrypts the data with the secret shared key of the destination and forwards it to the base station in multi hop fashion. HEED protocol is used in this approach for clustering process along with replicated mobile agents to prevent the sinkhole attacks in WSN. And mobile agents are used for alerting the nodes about their trusted neighbors so that they will not listen to the malicious node. Here the work is examined in terms of packet loss rate, throughput, and end-to-end delay.

Intrusion Detection Based On Neighbor Information - An intrusion detection algorithm for detecting sinkhole attack in wireless sensor networks is proposed by Guangjie Han et al [4] which is called as Intrusion detection algorithm based on neighbor information of sensor nodes to detect sinkhole nodes (IDASA). This is a different method from the traditional intrusion detection algorithm. The effect of the sinkhole attack is analyzed in detail with great care. The proposed IDASA consists of three phases. First is recognizing the suspicious nodes in which it has two types of routing paths, shorter routing path, and longer routing path. Shorter routing path contains a simple routing path with only three sensor

nodes from source to destination. Here the intermediate node is the suspicious node. The longer routing path is a routing path that has min four sensor nodes. Neighbor info is used to detect or recognize suspicious node. The second phase is identifying sinkhole nodes, where number of interaction and the acknowledgments are used to decide if the suspicious nodes are sinkhole nodes. The final phase is removing sinkhole nodes from the network. The ID info of the sinkhole nodes is deleted from the routing table.

Novel Agent-Based Approach – A novel agent-based approach is proposed by Sina et al [3], where trusted mobile agents are used to detect sinkhole attacks in WSN. In this approach, mobile agents are used to informing each node of their trusted neighbors so that the node does not listen to the traffic from the compromised node. The algorithm used in this technique to detect and prevent the attack is designed in 2 phases. First is the network deployment phase where all the nodes in the network are scattered randomly. Based on the percentage value of the agents, the number of nodes is randomly selected by the central station for sending the agent packet. An agent node is created after which in order to create neighbor nodes matrix table, HELLO packets are sent to see the number of nodes in their frequency range, where even the malicious nodes can get included in the matrix. After the neighbor finding process is completed the neighboring matrix entry will have the ids of single-hop neighbor nodes, but the valid bit and agent bit will be still false. In the second phase, i.e. the network maintenance phase, the agents start, agent cycling where, before any information exchange it performs a three-step negotiation called as Trusting procedure between the agent and the node. If the node is trustable, then the interaction begins, or else it is considered as an intruder. When the neighbor node is trustable, after the agent returns to the original node, then its related valid bit becomes true in the neighboring matrix or remains false. Also if at all the neighbor node is an agent node, then its agent bit also becomes true. When the agent returns, the calculation of the signal strength is done. The neighbor node is removed from the neighboring list if the received signal is below the threshold value. If the agent bit of that node is false, then the neighbor finding process is performed again by sending it to a control packet, as it does not have an agent. Thus this approach, the detection rate is found through energy consumption, packet loss rate, throughput, and agent overhead.

Key Management Approach – A novel technique to isolate the sinkhole attack from the WSN is proposed by Prakash C Kala et al [5]. In the proposed technique, a basic configuration is used to deploy the sensor nodes in a finite area. The source and destination nodes are randomly defined. The AODV protocol which is a reactive routing protocol is used to select the path from source to destination by considering the hop count and sequence number. The source node sends the route request packet for which the nodes adjacent to the destination node replies with the route replies packet. The malicious node impersonates the identity of the base station and all the sensor nodes send their data to the malicious node instead of the base station. The base station distributes a unique key to all sensor nodes in the network by using the concept of Armstrong number, where Armstrong number is a unique number of 16 bits, produced from the combination of various colors and the final key is formed by concatenating each node's unique identification with this key. All the nodes while transferring the data to the base station, asks for the unique identification number. The original base station will be able to provide the identification number with the help of the Armstrong concept but the malicious node will not be able to provide the unique identification number. Then that node is detected as a malicious node which is removed completely from the network by using multipath routing. This is informed to all the nodes in the network by sending an echo message. A comparative analysis of existing methods by different researchers described above is shown in the below Table 1.

Table 1: Existing Sinkhole Detection Techniques

Approach	Proposed Solution	Advantages	Disadvantages
Anomaly Based Scheme(Tumrongwitta yapak, C et al [2009])	An anomaly based scheme, using received signal strength indicator (RSSI) is proposed for detecting sinkhole attacks. The proposed solution uses RSSI value and extra monitors for detecting the sinkhole attack.	It is lightweight scheme and does not require additional communication overhead	There is no instant attack. The sensor networks are assumed to be static. If attacked instantly after the network deployment, attack cannot be detected.

Approach	Proposed Solution	Advantages	Disadvantages
Message digest Algorithm (S.Sharmila et al. [2011])	The message-digest algorithm is proposed to detect the sinkhole attack in WSN by comparing the message digest of the data sent in the original route and the new advertised route.	Algorithm achieves authenticity and data integrity.	Only one computation is considered at a time and if one more is advertised then it is suspended till the previous one is completed. Computation cost and network throughput is not calculated. More amount of time and the power required to transfer the message in two paths.
Mobile Agent-Based Approach (Sina et al [2013])	A novel approach is proposed where trusted mobile agents are used to detect sinkhole attacks in WSN. The algorithm designed is carried out in two phases.	Memory overhead is reduced. Limited Energy Utilization. No interference of base station to use special keys.	Listen to network traffic continuously. Causes reduction in energy and rapid incapability.
Hop Count Monitoring. (Md. Ibrahim Abdullah et al [2015])	A scheme based on hop count monitoring for detecting sinkhole attacks in wireless sensor networks is proposed which uses a common technique of distance of the nodes from the base station.	It successfully detects the sinkhole attack when the node is far from the base station. Also detects the wormhole attack	The sinkhole node detection is not accurate when the malicious node is near to the base station, i.e. at one or two-hop distance If the detection technique is increased for a lower threshold value, then it introduces false detection.
Intrusion Detection Based On Neighbor Information (Guangjie Han et al [2015])	An intrusion detection method i.e. different from traditional intrusion detection is proposed for detecting and removing the sinkhole nodes in WSN with the help of neighbor nodes information.	Traditional security like cryptography is not needed, thus reduces computation complexity. Mobile agents are not required to detect sinkhole attacks.	If the sinkhole node varies between 0 to 30 then these nodes continuously grabs and drops off the packets received.
HEED Clustering Concept(Vishwas et al. [2016])	HEED protocol is used in this approach for clustering process along with replicated mobile agents to prevent the sinkhole attacks in WSN. And mobile agents are used to alerting the nodes about their trusted neighbors.	Using HEED protocol, the long-distance transmission is reduced. Energy is saved to a large extent because of inter-cluster communication.	Formation of the clusters results in significant overhead. Cluster heads nearer to the sink gets drained off soon.
Cross Layer Approach (ARYA I S et al [2017])	A cross-layer approach using mobile agents is proposed for detecting and preventing sinkhole attacks in WSN. In this approach, the cluster where the attack occurs is detected instead of a node	High detection accuracy. Communication overhead of the network is not increased.	More time and energy is consumed in network recovery, when an attack occurs near the sink. Re-clustering requires more time and energy.
Swarm-Based Algorithm **(**Nithiyanandam et al [2019])	The proposed solution uses a swam based algorithm called Artificial Bee Colony Algorithm for detecting the sinkhole attack in WSN.	The overall network performance is improved in terms of less energy consumption, less	The major drawback is that in the presence of a large number of nodes comparison of each node requires more time.

Approach	Proposed Solution	Advantages	Disadvantages
	The compromised node is found by comparing the node ID with the node ID's defined in the rule set.	packet loss, and high packet delivery ratio.	
Key Management Approach (Prakash C Kala et al [2020])	A novel technique is proposed to detect the sinkhole attack in WSN by mutual authentication using 16 bit long Armstrong number.	Reduction of energy consumption. Minimum packet loss. Reduction of delay time.	High power utilization of the network. Comparison may require more time.

5. CONCLUSION

The increased use of WSN in daily life has made it necessary to increase the security mechanisms in the implemented networks. When compared to traditional networks, WSN is more vulnerable to many attacks. A sinkhole attack is a destructive routing attack in wireless networks among all the major attacks. This paper contains the analysis of different techniques used for detecting and preventing sinkhole attacks in WSN. The advantages and disadvantages of each method or technique are found to be effective in different situations. Most of the techniques failed in low detection rate, high network overheads, and high communication cost. Thus reduced network overhead increased detection rate and energy-efficient should be the focus for future solutions.

REFERENCES

1. Abdullah, M.I., Rahman, M.M. and Roy, M.C., 2015. "**Detecting sinkhole attacks in wireless sensor network using hop count**". IJ Computer Network and Information Security, 3, pp.50-56.
2. Aryai, S. and Binu, G.S., 2017, October. "**Cross layer approach for detection and prevention of Sinkhole Attack using a mobile agent**". In 2017 2nd International Conference on Communication and Electronics Systems (ICCES) (pp. 359-365). IEEE.
3. Hamedheidari, S. and Rafeh, R., 2013. "**A novel agent-based approach to detect sinkhole attacks in wireless sensor networks**". Computers & Security, 37, pp.1-14.
4. Han, G., Li, X., Jiang, J., Shu, L. and Lloret, J., 2015. "**Intrusion detection algorithm based on neighbor information against sinkhole attack in wireless sensor networks**". The Computer Journal, 58(6), pp.1280-1292.
5. Kala, P.C., Agrawal, A.P. and Sharma, R.R., 2020, January. "**A Novel Approach for Isolation of Sinkhole Attack in Wireless Sensor Networks**". In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 163-166). IEEE.
6. Kesav Unnithan, S.L., Lakshmi Devi, C. and Sreekuttan Unnithan, C., 2015. "**Survey of Detection of Sinkhole Attack in Wireless Sensor Network**". International Journal of Computer Science and Information Technologies (IJCSIT), 6(6), pp.4904- 4909.
7. Kibirige, G.W. and Sanga, C., 2015. "A **survey on detection of sinkhole attack in wireless sensor network**". arXiv preprint arXiv:1505.01941.
8. Nithiyanandam, N. and Latha, P., 2019. "**Artificial bee colony based sinkhole detection in wireless sensor networks**". Journal of Ambient Intelligence and Humanized Computing, pp.1-14.
9. Sharmila, S. and Umamaheswari, G., 2011, July. "**Detection of sinkhole attack in wireless sensor networks using message digest algorithms**". In 2011 International Conference on Process Automation, Control and Computing (pp. 1-6). IEEE.
10. Tumrongwittayapak, C. and Varakulsiripunth, R., 2009, August. "**Detecting Sinkhole attacks in wireless sensor networks**". In 2009 ICCAS-SICE (pp. 1966- 1971). IEEE.
11. Vishwas, D.B., Chinnaswamy, C.N. and Sreenivas, T.H., 2016. "**Discover and prevent the sinkhole attacks in wireless sensor network using clustering protocol**". Int J Adv Res Comput Sci Technol, 2(4), pp.26-28