[1]Mona R

[2]Manoranjitham R

Localization and Detection of Sinkhole Attacks in Wireless Sensor Networks Based on Denial of Service (DoS) Attacks

JES Journal of Electrical Systems

Abstract: - A wireless sensor network (WSN) uses uniformly deployed and positioned sensors to regularly send sensed data to a centralized station. Sinkhole attacks, in which a malicious node draws packets from other legitimate sensor devices and drops them, are the main danger to the WSN network layer and continue to be a difficult problem on wireless sensor networks. Security becomes a major issue since these networks have limited assets including less memory, less energy, and less transmission capacity. Additionally, given the dynamic context in which they are deployed, they are vulnerable to a variety of Denial of Service (DoS) assaults, including wormhole, sinkhole, and black hole attacks. The most dangerous routing attack at the network layer is known as a "sinkhole assault," which directs all network traffic onto a fake path by sending false information under the impression that it is the quickest one to the server. We explore sinkhole attacks to prevent them, and this work proposes a method of detection based on the redundancy process. Messages are transmitted across multiple paths to the suspicious nodes. Upon a thorough evaluation of the response, the attacked nodes are ultimately verified. Finally, a simulation is run to evaluate the method's efficacy. Furthermore, the simulation indicates that the strategy might be somewhat successful. Finally, it draws attention to difficulties and offers a prospective viewpoint for identifying sinkhole attacks.

Keywords: Denial of Service; sinkhole; black hole attacks; wireless sensor network; Localization.

I. INTRODUCTION

In the future, wireless sensor networks will likely represent a major technical leap. They can be used for a multitude of purposes, such as environmental monitoring, tracking wellbeing, and military applications. WSNs are often made up of low-cost, tiny devices that are placed in public, unguarded, and unsupervised settings for extended periods to monitor and gather data. After that, a wireless link is used to report the information back to the base station. Because WSNs are susceptible to several types of assaults, security plays a crucial role in their design [1]. Any suggested security solution is therefore severely hampered by the resource-constrained nature of sensor networks. Proactive and reactive security solutions are the two primary subcategories of WSN safety products. Because WSNs have very high computing complexity, prevention-based systems cannot realistically leverage techniques like cryptography and verification. Furthermore, these systems are improper since they employ broadcasting media for transmission, which allows an adversary to readily obtain the encryption keys. Detection-based strategies make use of tools that can recognize attacks by analyzing the actions of the system. Based on the abilities of the nodes, WSNs can be divided into two types.

Two methods for identifying network sinkholes are provided in this paper [2]. The idea behind these strategies is that since paths to the base station that travel via sinkholes are more appealing and are therefore taken more often, the nodes surrounding the sinkholes burn up their energy more quickly than other locations.

[1] *Corresponding author: Division of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Karunya University, Coimbatore, Tamil Nadu, India. Email: monar@karunya.edu.in.

[2] Division of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Karunya University, Coimbatore, Tamil Nadu, India. Email: manoranjitham@karunya.edu.

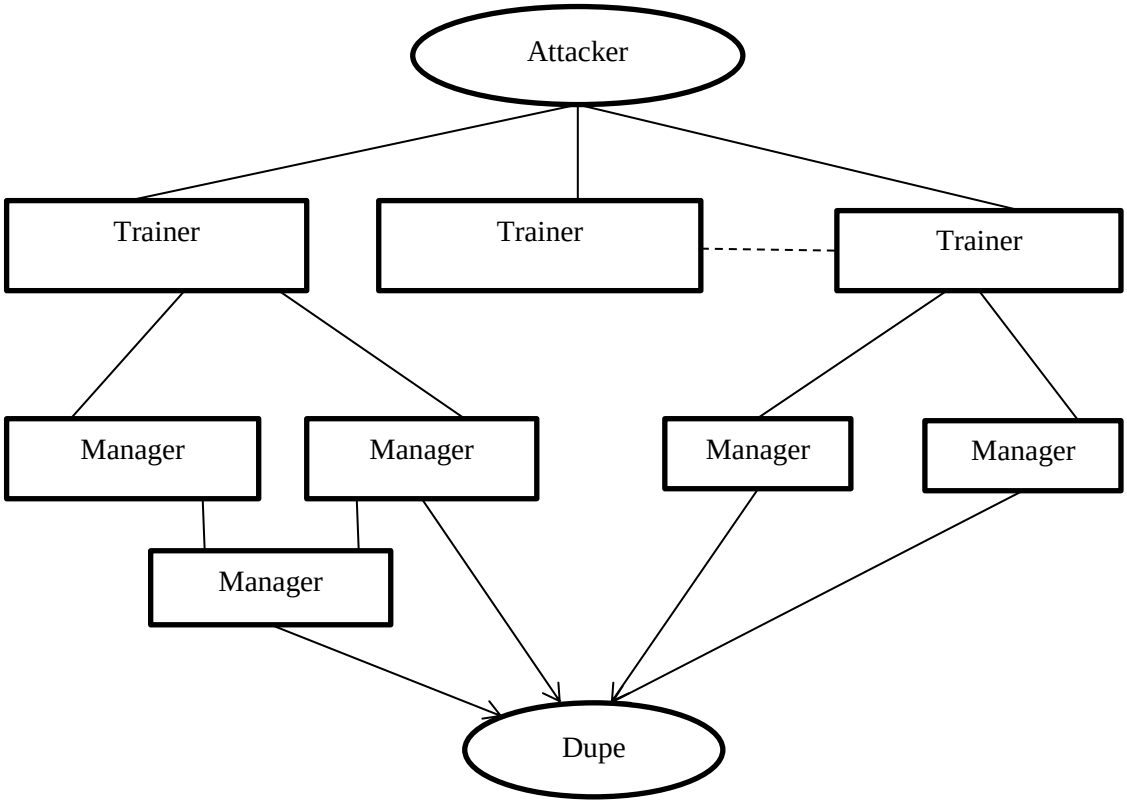

Figure. 1.1. The DDOS Attack Flow

Despite the abundance of DDoS literature, very few writers have taken the formal modeling of DDoS attacks in wireless sensor networks into consideration in Figure 1.1. Higher-layer systems are seriously threatened by sinkhole attacks because they keep the base station from getting accurate and full sensing data. Since wireless links are prone to failure, sensors are frequently placed in public spaces with limited processing power and battery life, making it especially bad for wireless sensor networks. Many of the current protocol stacks used in sensor networks are vulnerable to sinkhole attacks, even though certain secure or geographic-based routing systems are somewhat resistant to them [3]. Each sinkhole is surrounded by an energy hole as a result. In the primary technique, the base station samples the residual energy of each sensing zone using a geostatistical technique, and then uses an extracted statistical estimator to predict the likelihood that a sinkhole exists in each location. Based on the estimator's value, the base station instructs all nodes to avoid the questionable zone in their routing. The second approach finds regions with lower average remaining energy levels by using distributed monitoring. The following sums up our contributions:

- An estimate of energy holes has been proposed using a geostatistical risk model.
- Building on the suggested hazard model, we present a centralized model to identify sinkhole attacks.
- It has been suggested to use distributed monitoring to investigate each network neighborhood to find energy gaps.
- To represent how different contributing parameters interact in the proposed detection techniques, an analytical model is offered.
- We present a low-tech mitigating technique to close sinkholes.
- In conclusion, we offer comprehensive models to validate the acquired outcomes.

Since the sinkhole attack interferes with the victims' regular business operations, our suggested countermeasures to stop it might be seen as intrusion detection systems (IDS).

The remainder of the paper is organised in this manner. Section 2 presents the pertinent work. Section 3 presents the problem statement and a formal definition of the sinkhole attack in wireless sensor networks. We present the numerical analysis and improvements to the technique for managing many malicious nodes in Section 4 and the suggested algorithm's performance is assessed by simulations. This paper is finally concluded in Section 5, which also suggests some options for future investigation.

II. LITERATURE REVIEW

This section outlines the ideal framework specifications and points up issues with the existing related research. The first step of the literature research was to categorize the many systems and frameworks that already existed.

We developed a set of requirements that, if satisfied [4], enable a thorough and comprehensive study of suggested solutions in terms of their utility and efficiency. This allowed us to compare and arrange all of the current methods of denial-of-service formal modeling. For a modeling technique to be deemed valuable, functional, and effective, it must exhibit a specific set of attributes. While some concentrate on identification and mitigation techniques, others attempt to analyze distributed interruptions of service using various modeling methods.

An essential component of the WSN's availability is the nodes' use of the recommended security standards. Consequently, it's critical that academics deepen their understanding of the NesC programming language and the TinyOS operating system, which are prerequisites for creating applications for the networks. One of the security needs of the WSN, availability, is not satisfied by these protocols [5]. If the principle of availability is not given, it suggests that the protocol is vulnerable to denial-of-service attacks. It is also utilized in the WSN because of its low power fatigue, affordable price, and adaptability.

Five categories can be used to group existing systems and frameworks based on in-depth research and examination of relevant works. The five categories are outer blocking (OB), flash crowd (FC) assaults, low-rate DDoS (LR-DDoS) assaults [6], high-rate DDoS (HR-DDoS) attacks, as well as client validation (TB and CV) and traceback. Certain studies concentrated on how well the defensive system or framework could defend websites against high-rate DDoS (HR-DDoS) attacks, while others suggested that it should also defend against low-rate DDoS (LR-DDoS) assaults. According to some studies, it ought to offer defense against attacks by flash crowds (FC).

For example, the existing research on the flexible management of cyber-physical systems in Denial-of-Service assaults does not account for the uncertain state transition probability of the information layer, and the majority of studies on attack behavior are quite basic, focusing only on the scenario of a single kind of attack: CyberChemics system control problems [7]. A game-based H control strategy method is proposed in the literature along with an introduction to the security issues with CPS under DoS assaults. One approach is to think of the control performance as a zero-sum game and design mixed data layer strategies using performance counters; another approach is to think of both offensive and defensive approaches as a zero-sum random game and layout the system's physical controller using the best hybrid network tactics.

DDoS attacks are currently the most frequent and potent threats to organizations, and they are getting more and more alluring. For example, in 2018 GitHub was the subject of one of the biggest DDoS attacks ever [8]. One of the most well-known attacks of the contemporary era, this destructive one destroyed the basis of the presence component of the CIA safety triad. Attackers launch concurrent DDoS attacks using numerous dump devices, laptops, and botnets, depleting the target system's significant assets and stopping every service. DDoS attacks on both large and small targets can be carried out with a variety of legal and efficient technologies. There was just another DDoS assault.

In typical uses, localization techniques are essential for supplying data on the location of sensor nodes. They have been thoroughly studied in underwater sensor networks. We categorized localization techniques into three major categories: research article-based mobile, hybrids, and static algorithms [9]. In UWSNs, classification is dependent on the mobility of sensor nodes. Based on these classifications, the majority of research focused on methods for static node localization. All sensor nodes for the static localization procedure are fixed and steady in the specific chosen region, either fixed to the seafloor or attached to sea floats.

Collecting these reports and initiating an investigation into them is the responsibility of the node nearest that site. Every node participating in Space-Domain Detection (SDD) keeps a database in which it logs the data it has received from other nodes it has encountered in previous time units) [10]. Upon seeing one another and exchanging documented data on identity u, a portion of the witness nodes can discover inconsistent data that violates the lemmas. However each node in this approach needs to maintain an inverse hash chain and a set of notifications for each watched node. A sensor node might not be able to afford the storage cost.

III. METHODS AND MATERIALS

3.1 Sinkhole attack

To draw in neighbors and persuade them to take the advertised route more frequently, a sinkhole attacker node initially advertises the best possible route—one with the fewest hops—to the destination (BS). The effective advertised path that the sinkhole attacker node has declared can subsequently be used by the neighbors to forward their traffic. Other than the neighbor nodes of the sinkhole assailant nodes, which are not as close to BS as they are to the sinkhole, the path may also captivate additional nodes. As a result, the target node has the opportunity to change the data, obstruct regular network operations, or execute other dangerous actions [11]. Figure 3.1 depicts a sinkhole attack scenario of this kind.

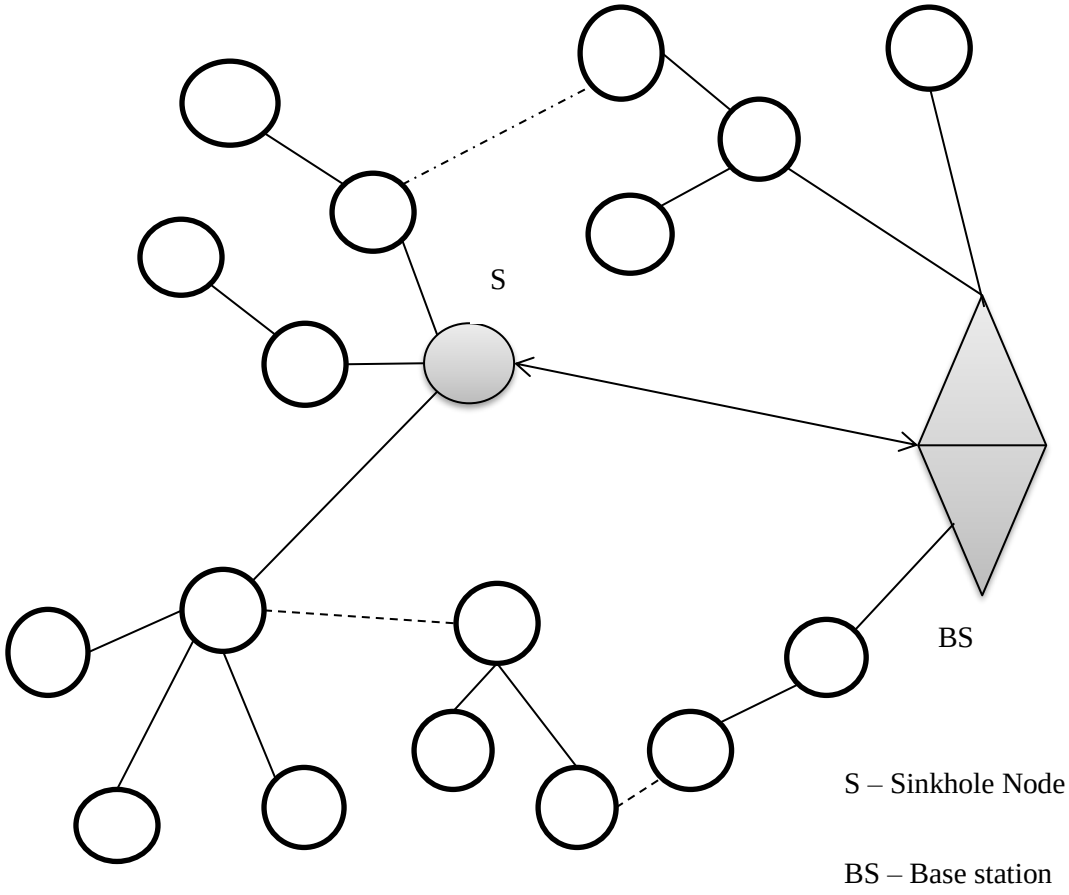

Figure 3.1. An example of a Sinkhole Assault Situation

There are three possible outcomes from a correctly deployed sinkhole attacker node: messages might be lost (it dropped by the intruder node), postponed, or altered. These three observations suggest the possibility of three different kinds of sinkhole attacker nodes:

- Sinkhole attacker nodes alter the messages before sending them to the following node, known as sinkhole message modification nodes.
- Sinkhole attacker nodes leak communications, sometimes even selectively, through sinkhole message dropping nodes.
- Nodes that induce a delay in communication forwarding are known as sinkhole message delay nodes (SDL) and are caused by potential attackers.

When sinkhole attacker nodes are present, messages can be discarded, altered, or delayed. This poses major risks to WSN operation since it prevents information from reaching the base station (BS) promptly and affects other network characteristics. In this work, we present a novel and effective detection scheme for three types of sinkhole attacker networks in HWSNs: SMD, SDP, and SDL. This is the initial attempt, as far as we are aware, to create a

sinkhole nodes detection method for HWSNs that can successfully identify SMD, SDP, and SDL attacker networks in Figure 3.2. Phases one and two comprise the suggested detection strategy. Sinkhole attacker nodes are identified in Phase 1 and their types (SMD, SDP, or SDL) are determined in Phase 2.

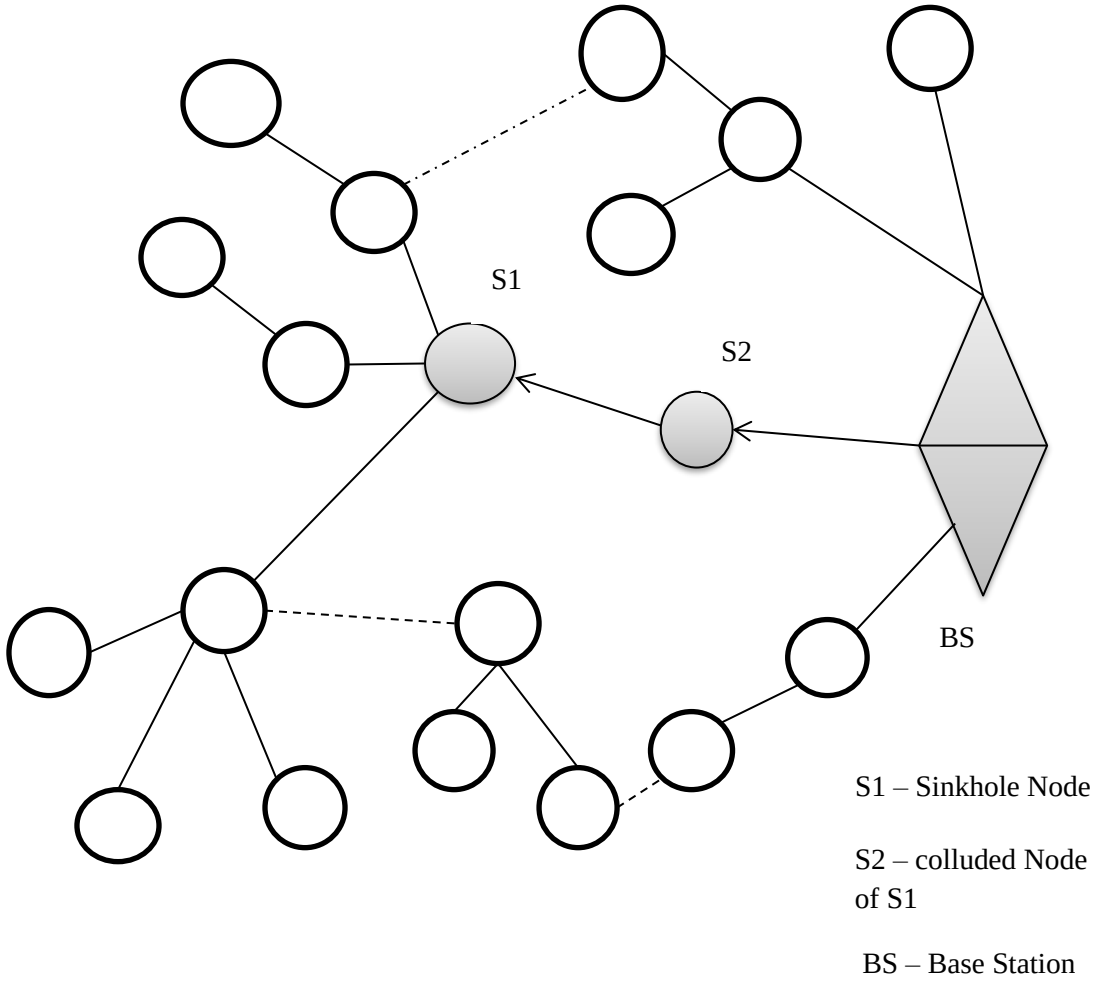

Figure 3.2. An example of a wormhole tunnel sinkhole assault situation

The wormhole attack can be used to mount the sinkhole attack. In this scenario, an evil node first gathers packets from its neighbors and then forwards them to another WSN colluding node, which is ultimately in charge of delivering the data to the BS, via a covert wormhole tunnel. It should be noted that, in contrast to other methods, the two ends of the wormhole tunnel may be farther apart. It does, however, stop the source from finding alternate routes that are more than two hops from the base station. Figure 3.2 depicts an attack scenario of this kind.

3.2 Detection of Sinkhole Attacks

In a sinkhole attack, the adversary aims to lure nearly all the data from a particular network through a compromised node, creating a virtual sinkhole where the opponent is positioned at the base station. In order to launch a sinkhole attack, a hacked node is typically made to appear extremely appealing to neighbouring nodes in terms of the routing system. Sinkhole attacks are challenging to prevent because it is difficult to confirm the routing details that a node gives. The adversary laptop class, for instance, is equipped with a potent radio emitter. This allows an opponent with laptop class to transmit data with enough power to cover a significant area of the network, hence offering a high-quality route. The adversary laptop class, for instance, is equipped with a potent radio transmitter. This gives the opponent with laptop class the ability to offer a high-quality path by using enough power to cover a significant area of the network through transmission.

We first concentrate on a single malicious node, and then in the following part, we improve it to discover several malicious nodes. Therefore, the programmer uses data consistency checks to first identify a list of suspected nodes, and then it uses network flow analysis to effectively identify the intruder in the list. Additionally, the method is strong enough to handle numerous malicious nodes working together to conceal the true invader.

3.2.1 Assess the area that was attacked

In the first approach, network flow data from the attacked region is gathered by the base station using a low-overhead, safe technique. In the second approach, the intrusive party is located and the routing structure is examined using an efficient identification technique. Furthermore, the intricate tale of collectively tricking the desired location about the invading condition through the use of cheating nodes is considered. These two techniques are applied to sinkhole attack targets in order to locate an intruder. Initially, the network is divided into multiple sub-domains based on the calculated attack area, and the data within each of them is compared. The attack may also be identified by looking for variable data among the usual sensors and attack nodes in the subdomains. Attackers cannot change the information starting at all the nodes in the system due to the size limits of the attacked region.

To illustrate, consider a supervision application based on the data that frequently arrives at the base station from node sensors.

Hence, the attack needs to be located in a few of the sub-areas. The BS can be used to determine the sinkhole's location after a cluster of suspicious nodes has been identified. Encircling a suspicious node or ability-attacked area is particularly possible. Second, there may be several nodes in the attack region, and in a multi-hop sensors system, the sinkhole is not always in the middle of the region. Moreover, it is not necessary to locate the precise intruder and cut it off from the entire network. In order to locate the intrusive party, one can assess the routing model within the impacted domain.

3.3 Dos attack types

One of the most common and serious types of attacks compromising network security is the denial-of-service attack, which can be described as any event that reduces or eliminates a network's ability to execute its expected function and degrades the network's intended service to its customers.

- **Jamming**

A malevolent node could be able to configure its radio to broadcast constantly or very often, jamming the radio receivers of its nearby nodes. The nearby nodes won't be able to receive transmissions since they can't understand any messages.

Defense: Using spread spectrum communications is the most popular line of defense against jammer attacks. When a device engages in frequency hopping, it sends a signal for a little while on one frequency, switches to another, and then repeats. Coordination between the transmitter and receiver is required. Direct-sequence spreads the information over a wide band, utilizing a pseudo-random bit flow [12]. A listener must know the propagation code to separate the signal from the noise.

- **Tiredness**

An attacker may potentially utilize a series of collisions to drain resources. Time-division multiplex could be one way to solve it. Setting rate limitations for the MAC admission control is a further potential remedy.

Rate-limiting response to even duly verified nodes is a defense. Requests that are too frequent will be ignored or queued up to avoid using costly radio communications. For authorized users, there needs to be sufficient speed and timely delivery at a high enough pace.

3.4 Attacks using Selective Forwarding

3.4.1 Wormhole assault

Through the use of a low-latency link, an attacker can tunnel messages received in one area of the network and replay them in another. A single node positioned between two other nodes transmitting messages between them is the most basic example of this attack.

Defense: based on package leashes, which restrict the maximum distance a message can go in a single hop. A timestamp and the sender's location are included in every message. If the maximum broadcast range has been reached, the receiver determines this by comparing it with its own location and time. The solution's applicability to WSNs may be limited by the need for precise location verification and clock synchronization.

3.4.2 Overflowing

The attacker can continuously request new connections until the resources needed for each connection are either depleted or exceed a certain amount. Any subsequent valid requests will be denied in either scenario.

Defense is to demand that service users invest a substantial amount of money before connections are made. One such technique is the distribution of cryptographic puzzles by servers, which need brute-force solutions before any connection-related server resources are allotted. Because the puzzles' complexity is scalable, the server can raise the bar if it senses an attack.

This could hurt the numerous valid sensor devices in a WSN, as they are all resource-constrained.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

After the results were analysed, the following conclusions were drawn.

- A single advertisement from a node can only be taken into account at a time. This means that if another node advertises while calculation is being done to determine whether or not that node is malicious, the previous advertisement must be ignored until that node's maliciousness has been established.
- In the impacted network, this technique can be utilized to identify several rogue sites.
- To find the malicious nodes [13], even very basic techniques for decryption and encryption are employed.
- Additionally, it recognizes selective forward attacks on reliable routing paths.
- It is vital to modify methods that will raise computation and communication expenses, such as hop count and connection quality identifier, in order to detect the advisory message level. The most effective approach for lowering the computation and communication overhead of the approaches without producing extra control packets is packet level identification.
- The shortcomings of the approach include the possibility that it won't identify a problematic node in the event of unclear collisions, low transmission power, fake misbehavior, and packet losses.

The efficacy of the proposed sinkhole detection system is assessed using the simulation of a wireless sensor network spanning 180 meters by 180 meters, where 400 nodes are distributed uniformly at random. To collect data from the sensors listed in Table 1, a base station is placed in the centre of the network. A sinkhole is additionally added to the system at the S and R coordinates (60, 60) in order to imitate a sinkhole attack. It's critical to evaluate how accurate intruder detection is crucial.

Table 1. Simulation Parameters

The quantity of nodes	400
The quantity of sinkholes	2
Drop rate of messages (d)	0.10
Dimensions of the packet	600
Sort of Traffic	GBR
Where the sinkhole is located	(25, 25)
Where BS is located	(60, 60)
Range of Gearbox	200m
Procedure	AOV
Evil node	2
Motion Model	Point Randomly

- **Precision of the intrusion detection system:**

The accuracy of the suggested intruder detection technique for sinkhole attacks is investigated in the first set of trials. Three measurements are considered: success rate: the proportion of instances in which the proposed algorithm properly detects the SH; false-positive rate: the proportion of instances in which the suggested method detects the SH wrongly, and false-negative rate, which indicates the percentage of times the algorithm fails to identify the intruder that actually exists. The functionality check looks into how well sinkhole attacks identify malicious nodes. The percentage of accurately detected sinkholes is represented by the success rate.

The percentage of sinkholes that are mistakenly detected is known as the false positive rate. The fraction of undiscovered sinkholes in the network is represented by false negatives. To determine precise rates, the system is run 1000 times. The configuration of the malicious node % is unpredictable.

The success percentage of identifying intruders is displayed in Figure 4.1. The graphic illustrates that the optimal conditions for the algorithm's operation are when m is less than 60% of cooperating nodes in dropping rate = 0.10. We may observe that the dropping rate decreases as it increases. This indicates that there are gaps in the networks' data.

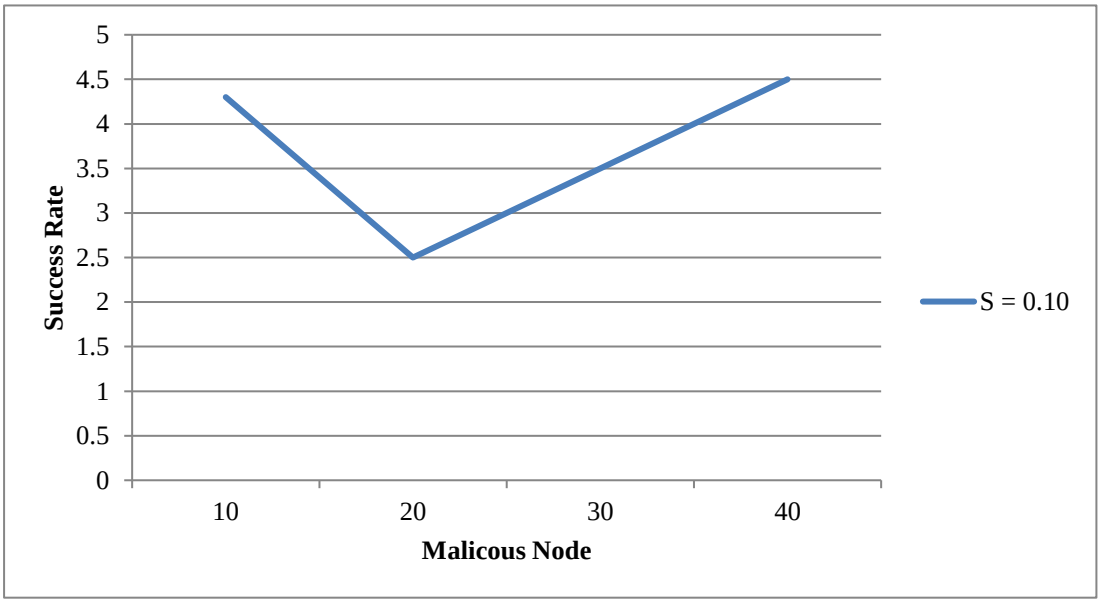

Figure. 4.1. Success Rate

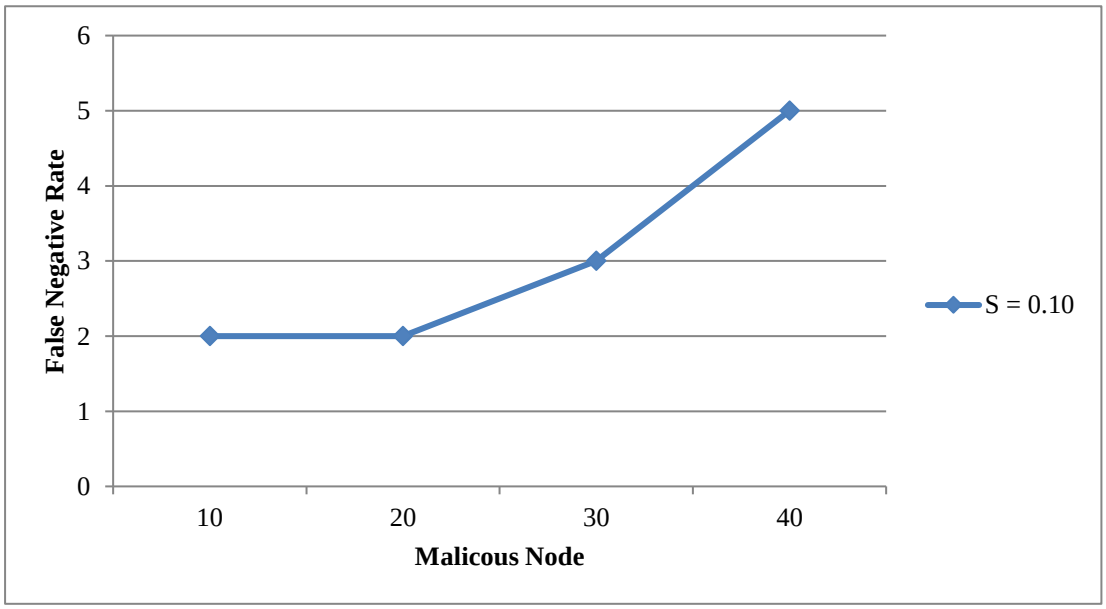

Figure. 4.2. False Negative Rate for Identifying Intruders

The false positive and false negative rates of conspiring nodes are displayed in Figure 4.2 [14]. We may observe that our algorithm performs well when the networks' false negative rate rises, while the rate of false positives is the opposite. The false positive rate increases somewhat to reach 43 when the cooperating nodes grow.

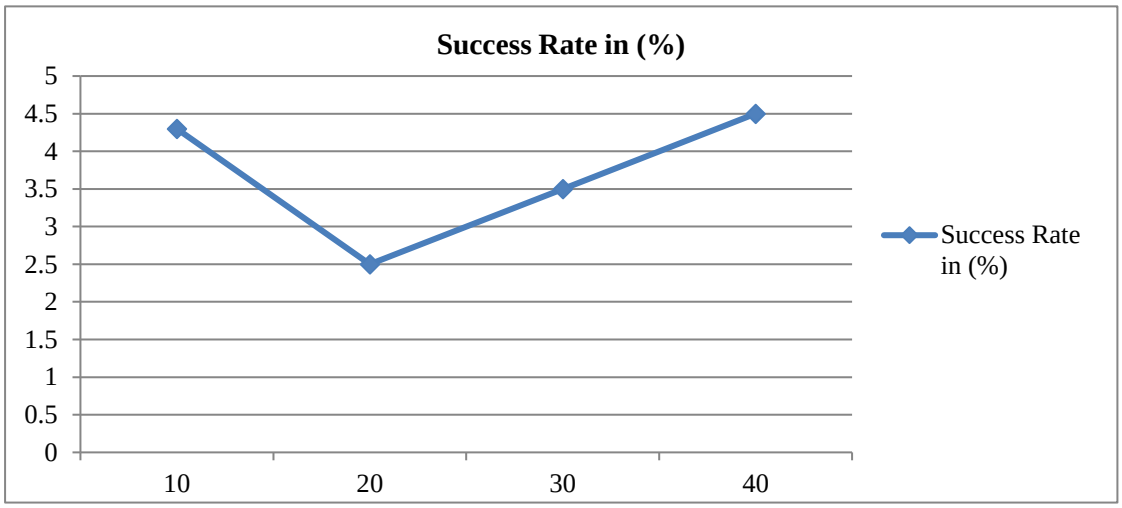

Figure. 4.3. Finds a False Sinkhole

The findings above demonstrate that our approach can effectively relate to earlier efforts in m=50% [15]. While our system achieves an 89% reliability rate in the end, compared to recent findings, the rate of cooperating nodes is marginally lower. Our method finds the intruder in 50% of cooperating networks at the highest accuracy rate in terms of intruder detection precision. Similar outcomes are displayed in Figures 4.2 and 4.3. This indicates that, in comparison to earlier studies, our method works in m=60% of colliding nodes.

V. CONCLUSION

This research proposes an efficient detection approach for wireless sensor network sinkhole attack detection. The algorithm in question, which consists of two steps, was suggested by this study as a worthwhile method for identifying sinkhole attacks in wireless sensor networks. The method first looks for a list of potential nodes by confirming that the data is consistent. The intruder on the list is then identified by examining the network flow data.

The fundamental requirements of a wireless sensor network are packet delivery promptly and security. Wormhole attacks, in which a malicious node dumps a packet and prevents it from reaching its destination, are the attack that has an impact on this. To satisfy the network's fundamental requirements, it is critical to identify these kinds of attacks.

In this paper, we address a few DoS attacks on wireless sensor networks, their effects on the network, and methods for defending against them. We also provide a list of detection techniques that will assist the user in understanding the methods that have been suggested recently and how new methods might be developed.

Aside from that, the study examined the algorithm's performance using simulations and numerical analysis. As a result, the algorithm's accuracy and effectiveness have been proven at the last section's outcome. More specifically, this study can be enhanced to identify data inconsistency using more effective statistical algorithms. To identify communication and computation overhead, they can thus accurately locate supposed nodes in sinkhole attacks.

REFERENCES

[1] Rassam, M. A., Zainal, A., Maarof, M. A., & Al-Shaboti, M. (2012, November). A sinkhole attack detection scheme in mintroute wireless sensor networks. In *2012 International Symposium on Telecommunication Technologies* (pp. 71-75). IEEE.

[2] Shafiei, H., Khonsari, A., Derakhshi, H., & Mousavi, P. (2014). Detection and mitigation of sinkhole attacks in wireless sensor networks. *Journal of computer and system sciences*, *80*(3), 644-653.

[3] Ngai, E. C., Liu, J., & Lyu, M. R. (2006, June). On the intruder detection for sinkhole attack in wireless sensor networks. In *2006 IEEE international conference on communications* (Vol. 8, pp. 3383-3389). IEEE.

[4] Mazur, K., Ksiezopolski, B., & Nielek, R. (2016). Multilevel modeling of distributed denial of service attacks in wireless sensor networks. *Journal of Sensors*, *2016*.

[5] Dener, M., & Bay, O. F. (2017). Practical implementation of an adaptive detection-defense unit against link layer DoS attacks for wireless sensor networks. *Security and Communication Networks*, *2017*.

[6] Saleh, M. A., & Abdul Manaf, A. (2015). A novel protective framework for defeating HTTP-based denial of service and distributed denial of service attacks. *The Scientific World Journal*, *2015*.

[7] Wang, Y., Hu, B., Pan, X., Xu, T., & Sun, Q. (2022). Security control of Denial-of-Service attacks in Cyber-Physical Systems based on dynamic feedback. *Computational Intelligence and Neuroscience*, *2022*.

[8] Esmaeili, M., Goki, S. H., Masjidi, B. H. K., Sameh, M., Gharagozlou, H., & Mohammed, A. S. (2022). Ml-ddosnet: Iot intrusion detection based on denial-of-service attacks using machine learning methods and nsl-kdd. *Wireless Communications and Mobile Computing*, *2022*.

[9] Ahmad, I., Rahman, T., Zeb, A., Khan, I., Ullah, I., Hamam, H., & Cheikhrouhou, O. (2021). Analysis of security attacks and taxonomy in underwater wireless sensor networks. *Wireless Communications and Mobile Computing*, *2021*, 1-15.

[10] Wang, Z., Zhou, C., & Liu, Y. (2017). Efficient hybrid detection of node replication attacks in mobile sensor networks. *Mobile Information Systems*, *2017*.

[11] Wazid, M., Das, A. K., Kumari, S., & Khan, M. K. (2016). Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. *Security and Communication Networks*, *9*(17), 4596-4614.

[12] Salehi, S. A., Razzaque, M. A., Naraei, P., & Farrokhtala, A. (2013, July). Detection of sinkhole attack in wireless sensor networks. In *2013 IEEE international conference on space science and communication (IconSpace)* (pp. 361-365). IEEE.

[13] Sharmila, S., & 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.

[14] Kaur, M., & Singh, A. (2016, September). Detection and mitigation of sinkhole attack in wireless sensor network. In *2016 International conference on micro-electronics and telecommunication engineering (ICMETE)* (pp. 217-221). IEEE.

[15] Ghildiyal, S., Mishra, A. K., Gupta, A., & Garg, N. (2014). Analysis of denial of service (dos) attacks in wireless sensor networks. *IJRET: International Journal of Research in Engineering and Technology*, *3*, 2319-1163.