E-ISSN: 2706-8927
P-ISSN: 2706-8919
www.allstudyjournal.com
IJAAS 2024; 6(11): 102-108
Received: 12-09-2024
Accepted: 18-10-2024

Jagathese G Chelladurai
Research Scholar
Department of Computer Science, Mansarovar Global University Bhopal, Madhya Pradesh, India

Dr. Mona Dwivedi
Research Guide
Department of Computer Science, Mansarovar Global University Bhopal, Madhya Pradesh, India

Corresponding Author:
Jagathese G Chelladurai
Research Scholar
Department of Computer Science, Mansarovar Global University Bhopal, Madhya Pradesh, India

Detection and prevention of wormhole attack in wireless sensor networks

Jagathese G Chelladurai and Mona Dwivedi

DOI: https://doi.org/10.33545/27068919.2024.v6.i11b.1473

Abstract
Wireless sensor network detection is compromised by a wormhole. In this study, we propose a technique to identify wormhole invasions in wireless sensor networks. Wormhole attacks are particularly challenging to defend against since the attacker doesn't have to compromise any nodes and can send packets on channels with low latency utilizing wireless gadgets like laptops and cellphones. In recent years, wireless sensor networks (WSNs) have become one of the most significant research areas in computer science, in part due to the challenging issues that these networks and their diverse variety of applications have raised. For the same reason, security on these networks, however, becomes a major concern.
Due to limitations in their computing capabilities, memory capacity, battery life, processing power, and tamper-resistant packaging, wireless sensor networks are susceptible to a number of internal and external attacks. Comparisons with a number of related techniques from the literature, such as Wormhole Detection Neighborhood Information, Authentication of Nodes Scheme (ANS), Received Signal Strength (RSS), and Wormhole Detection Using Hound Packet (WHOP) using the NS-2 simulator, are used to validate the proposed detection method. Based on simulation results, regional routing techniques have a low False Detection Rate (FDR).

Keywords: Wormhole attacks, mobile adhoc network, security, wireless sensor network, denial of service

Introductions

Ad-hoc and sensor networks are emerging as attractive platforms for a range of defense and non-defense uses. These networks are especially desired when setting up extensive networking equipment is impractical or expensive. Initial research focused on creating and realizing these networks by emphasizing their functional components, such as routing protocols and data aggregation techniques.

While there are numerous advantages to smart technology, the key obstacles are security and privacy since there are security risks associated with the large-scale deployment of sensor networks for various purposes. The mobile nodes work together to efficiently route data because the majority of sensor networks are often placed in uncontrolled situations without a central authority to oversee them. Mobile sensor networks are susceptible to a variety of routing-related security vulnerabilities because of their mobility, lack of a centralized authority, and scarce resource availability. In addition to other factors of relevance, such as energy efficiency, scalability, and QoS, the significance of security and privacy for components, including sensor networks, was described in [1]. Critical infrastructures including utility networks, communication and sensor networks, transportation networks, and more are provided by cyber-physical systems and the Internet of Things. The interaction between CPS, NCS, and WSN highlights the significance of WSN and its defense against assaults that compromise the performance and dependability of networks since it is a vital part of these systems.

Due to increasing complexity and a distinct multi-layer control plane, a centralized software-defined architecture widens the attack surface. It must confirm that the flow directives originate from legitimate sources. The connection between the switch and the controller, as well as different applications, are among the attack surfaces. Controllers are conceptually a single logical point of failure. The concentration of control logic in a single logical block also makes a centralized controller takeover catastrophic. The discovery protocol flaw can be used to strengthen an attack against the controller.

Additional security issues it raises include data leaking via timing analysis and unwanted access to the data and control planes of networks (wormhole attacks). Additionally, attackers have the ability to change network device rules, use compromised programs to change system settings, and launch a denial-of-service attack (DoS) (i.e., flooding control and data packets). A wormhole attack [?] is a particularly difficult security issue because, as long as the communication channel is known, it may be secretly deployed without jeopardizing other security measures. Wormhole attackers tunnel through their implicit direct communication linkages to draw data packets into one place and replay them at distant sites. By selectively dropping, flooding, recording, or altering packets, the attackers can also carry out a variety of malicious data and traffic manipulations without disclosing their identities. For wired networks, most of the current solutions against wormhole attacks make use of network topology data. Additionally, they employ high-tech tools like directional antennas, GPS, ultrasonography, and precise timing devices to attain a specific level of precision. However, the cost of those gadgets makes it impossible to use the resource-constrained HIoT nodes. In a software-defined HIoT, it is essential yet difficult to develop wormhole attack defenses since they depend on the network architecture, proximity to key neighbors, and geographic location.

Background

A black-hole attack happens when a router deletes all the communications it was supposed to forward. A router can occasionally be set up incorrectly to provide a free path to every Internet destination. This routes all traffic through the chosen router. The router fails because no device is able to sustain such a load. Wireless communication channels are vulnerable to a range of security attacks because to their open design, lack of infrastructure, quick deployment techniques, and potential placement in hostile environments. The wired domain's particular cryptographic primitives control these dangers, which may entail eavesdropping, message tampering, or identity theft [1]. Alternately, attacks like black hole and rushed assaults may target wireless network control or data transmission. It is generally more difficult to recognize and defend against such attacks than in wired configurations because many multichip wireless systems are resource-constrained (e.g., bandwidth, power, or computing). The wormhole attack, a very serious security breach, was carried out on adhoc networks [2]. This attack involves a malicious node capturing packets from one part of the network, "tunneling" them to another hostile node further away, which then changes the packets locally. The tunnel may be created using a concealed channel (such as a wired link), packet encapsulation, or high-powered transmission, among other techniques. As a consequence, compared to packets sent over standard multichip channels, tunneled packets arrive either quicker or with fewer hops. This gives the impression that the two ends of the tunnel are similar. It could be useful to use a wormhole tunnel to forward all packets. Ad-hoc and sensor network routing methods [3] are sabotaged in their malicious version by using nodes.

Motivations

It may be used by two nefarious tunnel endpoints to change routing so that they can draw routes through them. They may then carry out a range of attacks, including picking and choosing which data packets to discard, on the data traffic moving through the wormhole. The wormhole attack will stop two nodes from recognizing lawful routes beyond two hops, which will stop the network from functioning. Depending on the area, it may also have an impact on wireless security systems, data aggregation, and clustering. Last but not least, a wormhole attack may be launched without compromising a real network node or gaining access to any cryptographic keys [4].

WSN routing is difficult as a result of distinctive qualities that set WSN apart from other wireless networks, such as Mobile Ad Hoc Networks. Traditional IP-based techniques for WSNs are inapplicable due to the vast number of sensor nodes installed non the network. A particular base station is where the bulk of sensor network apps send their information. Sensor nodes need particular resource management because to their constrained battery, storage, and computation capability. In contrast to conventional wireless networks, almost all WNS nodes are either permanent or have very little mobility after installation [5].

WSN sensor nodes require specific hardware (such as GPS) to locate other nodes due to location-based data collection. Repetitive data during data collection must be removed for routing strategies in WSNs to consume more energy and bandwidth. Despite the fact that WSNs have made great strides in recent years, researchers are now concentrating more on creating a dependable routing system. Multiple attacks compromise the security of routing protocols in WSNs, leading to a range of problems such routing protocol change and a threat to the confidentiality, availability, and integrity of the conveyed packets, among other things.

Selective routing, sinkholes, sybil, wormholes, hello flooding, and spoofing are examples of security risks to WSNs. The wormhole assault, however, poses the greatest threat to a network's sensory shouldn't be put at risk. The Sybil attack, for example, may easily be started using the wormhole attack. Furthermore, cryptographic techniques cannot prevent wormhole assaults [6].

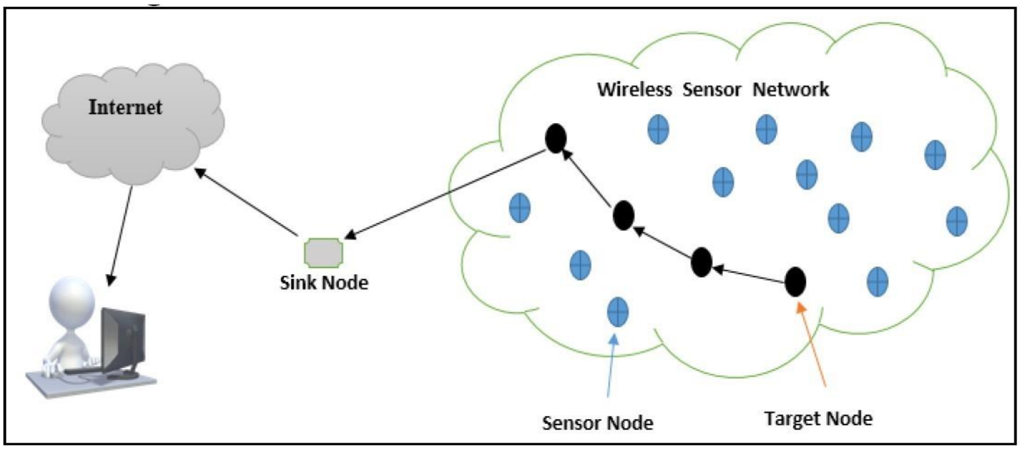

Fig 1: Architecture of Wireless Sensor Network

In recent times, wormhole attacks on wireless ad hoc networks have been attempted to prevent. These methods frequently use wormhole indications to pinpoint attacks. However, the majority of current methods necessitate either specialized hardware parts, such as radio transceiver modules or GPS directional antennas, or robust network presumptions, such as a precisely synchronized clock, guard nodes, unit disc communication models, or secure, attack-free environments [7].

The application of approaches in regional routing protocols, which include a high number of sensor nodes with constrained resources, is constrained by the use of such criteria and assumptions. Infrastructure-less architecture (i.e., no gateways are present, etc.) and the inherent requirements of WSNs (e.g., unattended working environment, etc.) may offer a variety of vulnerabilities that may attract attackers [8]. Security is a major issue when using WSNs for uses like the military and healthcare. Due to their special characteristics, WSNs will render conventional computer network security measures useless (or less effective).

Network intrusions will thus occur as a result of the lack of security measures. Recognizing these incursions is necessary, as is the implementation of defenses. Security improvements for wireless sensor networks. Omnidirectional antennas are found in the majority of wireless embedded networks, allowing neighbors to hear node-to-node conversations [9]. This was used to build a simple "local control" that could detect sophisticated attacks like wormholes and black holes, which almost completely eliminated the throughput of a sizable network [10].

Challenges in Wireless Sensor Network

1. Wireless Communication Nature
2. Unscheduled Deployment
3. Hostile Environment
4. Resource limitation
5. Unreliable Communication
6. Scalability
7. Absence of a Primary Coordinator

Related Works

Jaydip Sen and others Their routing protocol is AODV, and their simulation tool is ns2 simulator. They start out by going through the practical presumptions that were applied when building the network model. To find any malicious gray hole nodes in the network, the proposed method combines local and cooperative detection. The system consists of four security mechanisms that are gradually activated. The security approaches are: (1) Neighborhood data collection; (2) Local anomaly detection; (3) Cooperative anomaly detection; and (4) Global alarm raiser. Each node participates in local data gathering, which uses packet overhearing to identify any suspicious nodes nearby. In the event that one is found, the detecting node starts the local detection process to evaluate whether the suspicious node is an evil gray hole node. The initial detection node then starts the cooperative detection approach by broadcasting to all of the suspect node's one-hop neighbors, asking them to take part in the verification process to make sure the suspect node is really malicious. In order to build a sufficient warning system and inform the whole network, the global reaction is immediately activated upon the discovery of a confirmed gray hole node.

With the use of three linked algorithms and an aggregate signature technique, GaoXia openg proposed a method for locating packet-dropping nodes. 1) The proof-generating algorithm. Each node taking part in a session must produce a proof using the aggregate signature technique to prove that it has received a message. 2) The algorithm for verification. This method is used by the source node to identify the malicious node when it notices that a packet-dropping attack has taken place, such as when the destination reports that fewer packets have been received than would be expected under normal circumstances. 3) The diagnostic approach. Based on the data that the checkup method provides, the source node may be able to identify the malicious node. For simulation, the ns2 simulator is employed. According to simulation results, our technique is capable of identifying the majority of malicious nodes, the cost of routing packets is cheap and the false positive rate is low, and the packet delivery rate has increased. As evidence on forwarded packets is used, the dependability is acceptable, the application scope is large, the security is satisfactory, malicious nodes cannot easily evade detection, and the bandwidth overhead is minimal since nodes do not need to keep track of one another.

The AODV routing protocol is employed by Megha Arya and others. They updated aodv to "gray hole aodv" and provided ids aodv (Intrusion Detection System AODV), which is a variant of gray hole aodv, to demonstrate the Gray Hole Attack by inserting a malicious node that depicts a gray hole. For simulation, we employ the NS2 simulator. Based on simulations, this study comes to the conclusion that IDS can be used to restore Throughput, Routing Load, and Packet Delivery Ratio in the case of a Gray Hole Attack.

In order to distinguish gray hole nodes from normal nodes with a greater sequence number, A. M. Kanthe *et al*. developed a method. Whether or not the reply packet sequence number is less than the peak value is determined and verified by the algorithm. The following variables are used to calculate the peak value:

a) The routing table sequence number
b) The reply packet sequence number.
c) The ad hoc network's elapsed time, which relates to the simulator's present simulation time in the simulation environment.
d) The quantity of reply packets that the replying node or intermediary node has received. The replying node's RFR (Reply Forward Ratio).

For instance, the approach recommended by D. G. Kariya *et al*. is based on a system of courses. In this approach, a node only sees the subsequent hop along the current route path, but it keeps track of all of its neighbors. Each node in this technique keeps a Fwd Packet Buffer, commonly referred to as a packet digest buffer. There are three steps in the algorithm:

A) The detecting node hears the packet's digest when it is transmitted since it is saved in the Fwd Packet Buffer.
B) The Fwd Packet Buffer will release the digest as soon as the next hop advances the packet is detected.
C) Within a specific period of time, the detecting node must compute the overhear rate of its subsequent hop node and compare it to a predefined threshold. The hearing

Mr. Chetan S. Dhamande *et al*. presented a strategy for reducing the impact of gray hole attacks using the AODV routing protocol. The waiting time for the source node to receive the RREQ from other nodes is first set, and then the current time is added to the waiting time. Once the calculated time has passed, preserve the RREQ Destination Sequence Number (DSN) and associated Node ID in the RR-Table. The initial entry in the RR-Table is often kept as the first route reply, which typically comes from a malicious node with a high destination sequence number. Then, compare the source node sequence number with the original destination sequence number; if there are several inconsistencies, the node is obviously malicious; immediately remove its entry from the RR-Table. This is how harmful nodes are located and eliminated. The last step is selecting the subsequent node id with a higher destination sequence number, which is obtained by sorting the RR-Table according to the DSEQ-NO column, which packet is transmitted to malicious node detection in order to carry on with the AODV protocol's default operations.

By rejecting the first shortest path for data packet transmission and choosing the second shortest path, Hizbullah Khattak *et al*. provided a method for preventing black/gray hole attacks. As a result, sending the RREP message again is difficult for the rogue node. A malicious node must keep track of the whole network in order to be a part of the second shortest path, which is obviously difficult in a MANET. They also recommended the hash function for data integrity and detecting these two attacks in order to boost safety and security. The majority of defenses stop lone blackhole or grayhole attacks, however this defense also guards against group blackhole and grayhole attacks. The recommended method improves the security and dependability of AODV's data packet transport.

In order to eliminate black holes, a solution that modifies the basic AODV routing protocol was proposed by Latha Tamils Elvan and Dr. V Sankara narayanan. It is advised to wait for and review the replies from all nearby nodes before deciding on a safe path in order to reduce the chance. The inquiring node must hold off on sending the DATA packets to the reply node until other nearby nodes answer with next hop information, according to the suggested technique.

Once the first request is received, a timer is set up in the Timer Expired Table to collect additional requests from other nodes. The "Collect Route Reply Table" will be used to store the packet's "sequence number" and arrival time (CRRT). Each node's waiting time varies in direct proportion to how far it is from the source. Depending on the time the original route request arrives, it chooses the "timeout." The CRRT is checked to determine whether there is a recurring next hop node after the timeout value. It assumes that the pathways are valid or that the chance of malicious pathways is minimal if there is a repeated next hop node in the reply pathways. Then, any of the paths, including the repeating node, are used to send the DATA packets.

Proposed architecture

The network's performance is impeded by the presence of malicious nodes. This malicious node connects to the network and launches wormhole and black hole attacks. One of the most common active attack techniques, known as a sinkhole, involves an attacker node flooding the network with erroneous packets while the sensor node is kept busy sending the route packet reply. This study recommended the isolation of harmful nodes upon network entrance. The steps in the process are as follows:

Step1: There are a limited number of sensor nodes in the network. Step2: While loop will be run in every network node.

1. The base station will determine the location of the node by utilizing the node localization method.
2. The base stations assign an individual Armstrong number to each node.
3. Each node is also assigned a unique ID by the base stations.

While EndStep3: The development of cluster heads begins in the networks.

1. The cluster head is selected in the network on the basis of distance and energy
2. The unique ID, Armstrong of volunteer nodes are then send to the base station.
3. Execution of loop take placace. Step3.1
    1. All information corresponded
    2. The selected nodes are cluster heads
    3. Else Node gets isolated

Sensor nodes in a WSN are a self-configuring network structure that gather data and send it to the base station. Numerous active assaults of various types are possible depending on the network type. The sinkhole attack is difficult to distinguish from the network due to its distinctive features.

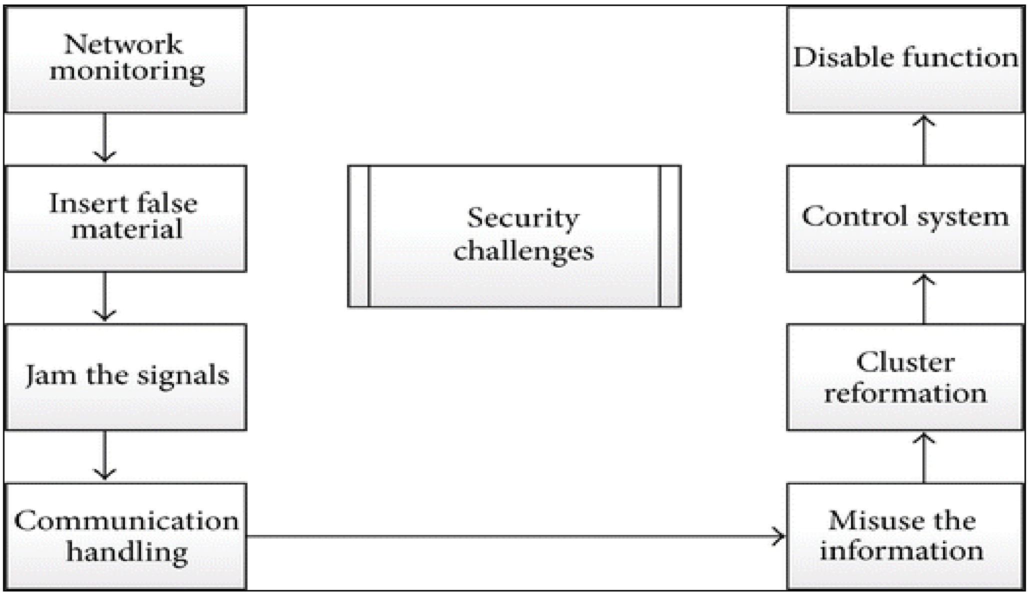

Fig 2: Proposed System Architecture

Detection Accuracy

When two or more nodes in a WSN have the same ID, it is possible to calculate the chance of an accurate identification of a mobile duplicate (identity). False positives in a WSN relate to faulty replica detection whereas true positives refer to effective node replica identification. The efficiency of replica detection techniques is decreased by false negatives, which show that the duplicated node is not recognized as a clone. A high positive rate (nodes successfully detected) and a low false positive rate (false positives) are desirable in a detection technique (normal node is accused).

Memory Overhead

Information on clone attack detection must be stored, checked, and compared by each mobile node (i.e., if same node identity is found). Because of this, each node has to have enough memory to store data or information (i.e., node Identity, node key, location, etc.). a mobile node's likelihood of absorbing energy while sending and receiving messages. Replica contact costs for detection must be sufficient and reliable. Progress Rate (Fast or Slow) The speed at which a possible danger is discovered is related to the likelihood of detection rate. The probability of detection times shows that the offered approach found duplicates quickly, effectively, and efficiently. An attacker might, alternatively, intercept the entire transmission using late detection. Consequently, network protection may be separated into two stages: rapid detection and gradual detection.

1. Is subject to the MWSN replica attack detection techniques. If a rapid, fast, speedy, and quick detection system is employed, the network will be protected against hostile activities very successfully. Today, the main emphasis is on rapid detection methods for mobile replication assaults (1).
2. Slow detection: We found that while several suggested strategies for replica detection assaults in MWSN exist, none of them make use of quick detection methods. As a result, if detection takes a long time to complete, an attacker may have time to watch the whole network connection for malicious activities. Replicated node assaults often go through two phases: a hazardous period and a non-hazardous phase. If the attack is not serious, the network will be shielded from the attacker's damaging threats even with a slow detection rate. The network would not be protected in the alternative, and network defense would be exceedingly hazardous and difficult.
3. Environment-based embedded sensors continually assess a person's physical state to diagnose their health. These sensors could make use of sensing floors, depth cameras, or other data sources that offer comparable information. Body-area networks may gather data on an individual's health, level of fitness, and energy consumption. When sensor networks are connected to the Internet of Things, user identification becomes more difficult, but new research has provided a solution. Wireless sensor networks are composed of unattended, low-power, small, and short-range sensor nodes. Recent observations have been achieved by irregularly turning on and off the sensing and communication capabilities of sensor nodes.

Results and Discussion

The ratio of the total number of network adversary attacks to the total number of recognized wormholes is known as the rate of wormhole detection. The detection rate of wormholes in relation to tunnel length is shown in Figure 4.1. We place one wormhole at random in each cycle. All wormhole attacks may be detected by our system (DWGRP) (100 percent). The ANS system has a wormhole detection rate of about 80%. When the tunnel length reaches ten meters, RRS has a minimum wormhole detection rate of around fifty percent. When identifying wormhole assaults, DWGRP's output is frequently sufficient and superior to other approaches.

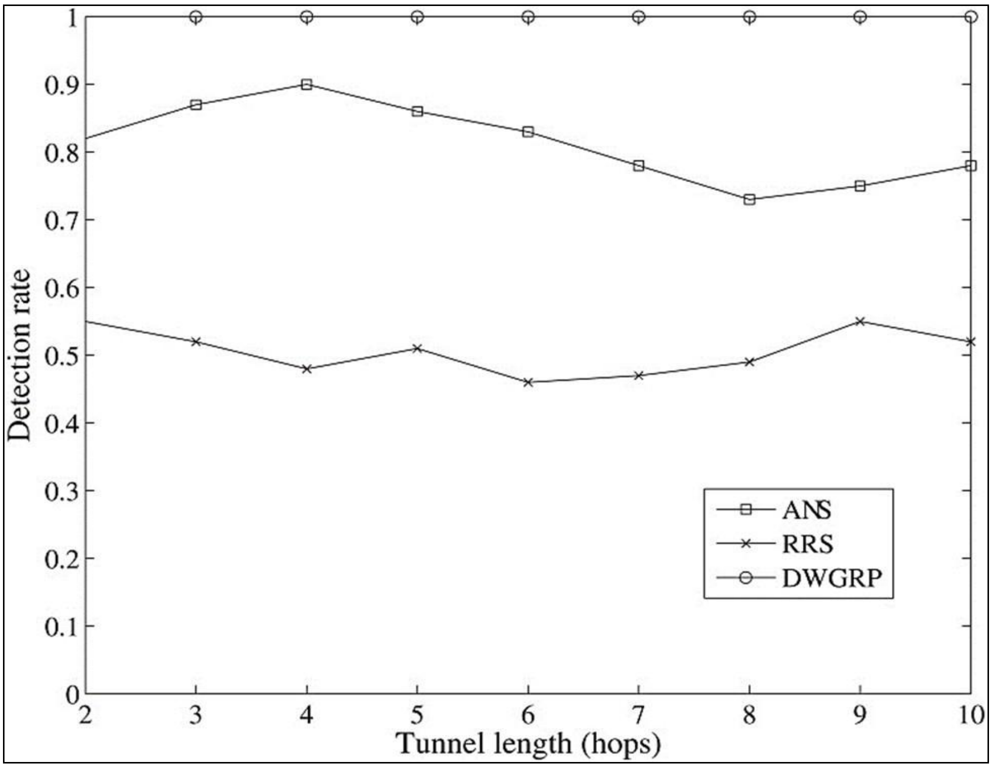

Fig 3: Worm hole detection rate in tunnel length

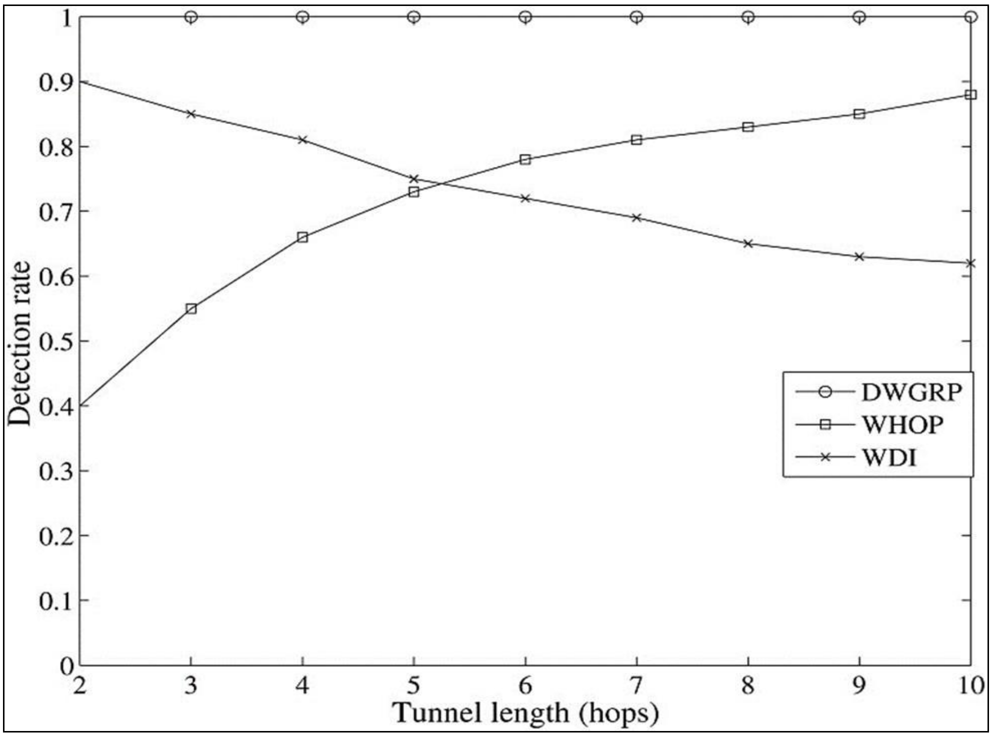

Fig 4: Worm hole detection rate

Then, we contrast our DWGRP method's wormhole detection rate with that of WHOP and WDI. To compare the results of the WHOP and WDI steps of the GPSR protocol, we simulate them. Figure 4.2 shows a slight negative trend in the WDI wormhole detection rate, with the detection rate dropping from 90% to 70% as tunnel time rises. In the WHOP system, the detection rate rises to almost 85% when the number of hops is increased to 10. In geographic routing protocols, our method outperforms WHOP and WDI because DWGRP can detect all wormhole assaults.

Conclusion

It is well acknowledged that wormhole assaults pose a serious threat to wireless sensor networks and routing technology. Wormhole attacks are difficult to recognize because they take many different shapes. We categorize wormhole attacks based on their characteristics and effects on different routing systems. We then offer a special method for identifying wormhole attacks in regional routing protocols by expanding the pre-distribution mechanism based on beacon packets. Prior to message receipt, our technology can detect malicious nodes. The suggested technique does not need any specific hardware or additional presumptions, such as network synchronization, unique guard nodes, or disc communication model units. Compared to work in spatial routing protocols or analytical modeling, simulation and modeling findings show that the DWGRP approach gives improved performance and applicability with fewer limitations. Future work will alter the paired key pre-distribution approach to better detect all rogue nodes. We'll also come up with a plan to prevent the Sybil assault.

The innovative wormhole countermeasure in HIoT is a Software-defined Wormhole Attack Analysis utilizing the Neighbor Similarity (WAND) method. WAND detects wormholes without needing any specific location information and without adding a lot of communication or coordination cost by analyzing the similarity of neighbor counts at a centralized controller. The WAND algorithm additionally employs NSI and ACI parameters to mitigate different clever wormhole attacker model situations. The vast experimental findings demonstrate that WAND can effectively identify wormhole assaults in very complex attack situations.

References

1. Basagni S, Conti M, Giordano S, Stojmenovic I. Mobile Ad Hoc Networking. Hoboken: John Wiley & Sons, Inc.; 2004. ISBN: 0-471-37313-3.
2. Abdelaziz A, Nafaa M, Salim G. Survey of routing attacks and countermeasures in mobile ad hoc networks. In: IEEE 2013 UKSim 15th International Conference on Computer Modelling and Simulation; 2013.
3. Jhaveri RH, Patel SJ, Jinwala DC. DoS attacks in mobile ad hoc networks: a survey. In: IEEE 2012 Second International Conference on Advanced Computing & Communication Technologies; 2012.
4. Sen J, Chandra MG, Harihara SG, Reddy H, Balamuralidhar P. A mechanism for detection of gray hole attack in mobile ad hoc networks. In: IEEE; 2007. p. 1-6.
5. Xiaopeng G, Wei C. A novel gray hole attack detection scheme for mobile ad hoc networks. In: IFIP International Conference on Network and Parallel Computing; 2007. p. 420-425.
6. Sen J, Chandra MG, Harihara SG, Reddy H, Balamuralidhar P. A mechanism for detection of gray hole attack in mobile ad hoc networks. In: IEEE; 2007. p. 1-6.
7. Kanthe AM, Simunic D, Prasad R. A mechanism for detection of gray hole attack in mobile ad hoc networks. Int J Comput Appl. 2012;53:1-5.
8. Kariya DG, Kathole AB, Heda SR. Detecting black and gray hole attacks in mobile ad hoc network using an adaptive method. Int J Technol Adv Eng. 2012 Jan;2(1):1-4.
9. Dhamande CS, Deshmukh HR. An efficient way to minimize the impact of gray hole attack in ad hoc network. Int J Emerg Technol Adv Eng. 2012 Feb;2(2):125-129.
10. Khattak H, Nizamuddin, Khurshid F, Amin N. Preventing black and gray hole attacks in AODV using optimal path routing and hash. In: IEEE; 2013. p. 1-5.
11. Tamilselvan L, Sankaranarayanan V. Prevention of blackhole attack in MANET. In: 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007); IEEE; 2007. p. 21-26.
12. Arora N, Barwar NC. Evaluation of AODV, OLSR and ZRP routing protocols under black hole attack. Int J Appl Innov Eng Manag. 2014 Apr;3(4):239-244.
13. Arora N, Barwar NC. Performance analysis of black hole attack on different MANET routing protocols. Int J Comput Sci Inf Technol. 2014;5(3):3094-3097.
14. Arora N, Barwar NC. Performance analysis of DSDV, AODV and ZRP under black hole attack. Int J Eng Res Technol. 2014 Apr;3(4):1291-1294.
15. Arora N, Barwar NC. Performance analysis of DSR, AODV and ZRP under black hole attack. Int J Appl Res Eng Sci. 2014;1(2):34-39.
16. Dareshoorzadeh A, Taheri Javan N, Dehghan M, Khalili M. LBAODV: A new load balancing multipath routing algorithm for mobile ad hoc networks. In: 6th IEEE NCTT-MPC; Malaysia; 2008. p. 344-349.
17. Taheri Javan N, Dareshoorzadeh A, Soltanali S, Ghanbari Birgani Y. IZM-DSR: A new zone-disjoint multi-path routing algorithm for mobile ad hoc networks. In: 3rd European Symposium on Computer Modeling and Simulation (EMS); Athens, Greece; 2009. p. 511-516.
18. Clausen T, Jacquet P, eds. Optimized Link State Routing protocol (OLSR). RFC 3626. IETF Network Working Group; 2003.
19. Gupta R, Musacchio J, Walrand J. Sufficient rate constraints for QoS flows in ad hoc networks. UCB/ERL Technical Memorandum M04/42; 2004.
20. Schrijver A. Combinatorial Optimization: Polyhedra and Efficiency. Berlin: Springer; 2006.