# Prevention of Wormhole Attack Using Mobile Secure Neighbour Discovery Protocol in Wireless Sensor Networks


**D. Jeyamani Latha, N Rameswaran, M Bharathraj, and R Vinoth Raj**

**Abstract** Wireless sensor networks (WSNs) are vulnerable to various types of attacks, and one of them is the wormhole attack. The wormhole attack can severely damage the network by creating a tunnel between two distant nodes, enabling attackers to bypass the normal network routes and steal sensitive information. In this project, we proposed a prevention mechanism for the wormhole attack using the Mobile Secure Neighbour Discovery Protocol in WSNs. We implemented our proposed mechanism using the NS2 simulator and evaluated its performance against the wormhole attack. Our proposed mechanism uses a unique secret key between nodes to prevent attackers from creating a tunnel between them. By tracking the amount of time it takes for the messages to arrive at their destination, we implemented the Mobile Secure Neighbour Discovery Protocol in our system to look for wormhole attacks. Our simulation results show that our proposed mechanism is effective in preventing the wormhole attack in WSNs. It successfully detects and isolates the malicious nodes responsible for the attack, thereby ensuring the security and reliability of the network. Moreover, the proposed mechanism incurs minimal overhead and does not affect the network's performance. Our findings indicate that our proposed mechanism can be a useful tool for securing WSNs against the wormhole attack. And it enhanced network throughput, packet delivery ratio, false detection ratio, and reduced the delay, energy efficiency, and overhead.

**Keyword** SEND protocol · Overhead · False detection ratio · Tunnel

D. Jeyamani Latha (✉) · N. Rameswaran · M. Bharathraj · R. Vinoth Raj
Electronics and Communication Engineering, Velammal Institute of Technology, Chennai, India
e-mail: djl@velammalitech.edu.in

R. Vinoth Raj
e-mail: vinothraj@velammalitech.edu.in



P. P. Joby et al. (eds.), *IoT Based Control Networks and Intelligent Systems*, Lecture Notes in Networks and Systems 789, https://doi.org/10.1007/978-981-99-6586-1_15

## 1 Introduction

A wireless sensor network is made up of small sensor nodes that operate autonomously. As a result, it was subject to several attacks, including, Byzantine, denial-of-service, tampering attacks, eaves dropping, node replication, sink hole attacks, and Hello Flood attacks. A wormhole attack is a difficult activity that affects how well wireless sensor networks operate. The use of wireless sensor networks to address difficult security attack issues continues to draw interest from commercial and scholarly research initiatives. Wormhole attacks are one of the most difficult security issues in wireless sensor networks, interrupting the majority of the routing protocols in many ways. In this technique, an attacker intercepts data packets at one network point and tunnels them to another, where they are then delivered back into the network. Wormholes are the names for the passageways created by two attackers working together.

Wormhole attacks can be prevented by secure routing protocols, cryptographic techniques, time synchronisation, physical layer techniques, detection algorithms, and localization techniques. These methods are also helpful in stabilising wormhole attacks. Various types of security attacks in wireless sensor networks include wormhole attacks, sinkhole attacks, selective forwarding attacks, Sybil attacks, jamming attacks, physical attacks, and spoofing attacks. Here, the major concern is to prevent wormhole attacks. By implementing detection algorithms, the network can identify the presence of wormholes and isolate the affected nodes or routes to minimise their impact on the overall network.

A wormhole attack may be formed using a single wired or wireless long-range communication link between the two conspiring attackers. Even for packets that are not directed at the attacker, a wormhole can be constructed because of the radio channel's broadcast nature. In this study, we use the MSND protocol to defend against this difficult attack. Between the source node and the destination node, a wormhole forms. Every node in the network wormhole that a source node can reach is first informed of the source address and data packet, and only then does the source node tunnel the data packet through another node. Therefore, since the destination cannot receive data packets and the source node continuously sends the information, it may be a risky situation where important and secure information may be split.

## 2 Related Works

Secure Neighbour Discovery (SEND), which involves a variety of ethics and technology, is explored in [1]. Several strategies were put forth to deal with SEND generally and wormhole attacks specifically. Many strategies make use of the physical characteristics of communications and can be generally classified in ways based on place, time, place and time, and network geometry. In order to confirm that nodes

claiming to be neighbours indeed live in the same neighbourhood, other location-based solutions provide neighbour discovery procedures. Time-based solutions make an effort to affect time-of-flow measurements to make sure that transmitting nodes are situated near other nodes in the immediate area. One well-known example of this strategy is pack leashes.

A location-based solution defines the neighbourhood and shares the same neighbourhood. Priyantha [2] proposed using both an ultrasonic emitter and an RF packet to accurately tell where the node is located. A time-based solution offers time of flight measurement to detect that the sending node is present in local areas. Hu [3] suggests a method to calculate the time and distance between the flows of data packets. Geometry-based solutions explain the detection of wormholes present in networks. Using flooding, count the hop distance between the nodes by Xu [4]. That structure can be used to detect wormholes. Connectivity graphs find the forbidden structure of wormholes as proposed by Maheswari [5]. Finally, how the attacker can be founded and how to reduce the capability of the attacker are suggested by Liu [6].

One solution that is frequently used is data-centric routing. Here, sensor nodes broadcast an advertisement outlining the data that is available and then hold off on sharing the data until a neighbour requests it [5]. WSN is adaptable in terms of simplicity of deployment and numerous capabilities due to its lack of infrastructure. Yet this also leaves it open to attacks and security issues. In order to collect or respond to active frames, an attacker may use an in-band or out-of-band channel to build a tunnel between two remote points in the network. Two distant nodes appear to be near one another thanks to the wormhole tunnel [7].

The foundation of the MSND protocol is the notion that when nodes range while moving, the distance between subsequent ranges and the duration of the next range are connected. The wormhole is unable to effect ranging operations in a way that would change the consistent set of ranges that must be established since it is unable to determine the distance travelled by each node. The key to this concept is graph rigidity. One can specify a node's course of travel in relation to another when two nodes follow definable paths. The directions of travel may be parallel, convergent, or divergent. There are an infinite number of possible connections between the two ranges. While a hard graph results from four or more ranges, three ranges only allow for a small number of discrete scenarios in terms of relative pathways. The predicted lengths of the following ranges can be precisely estimated in this rigid graph, and they can be contrasted with the ranged value itself.

## 3 System Model

Wireless sensor, self-control and legacy network systems for emergency response and military applications model the system concept. In the nodes in MSND contain single radio transceiver having enough ranging and precision time. Ranging radius 0.5–1 m. Mobile nodes can calculate ranging with degree of some error. Nodes in the

protocol perform the crypto graphic operation with public or symmetric keys shared between the two nodes in bidirectional, symmetrical manner.

### *3.1 Threat Model*

Threat models are considered to be located in geographic regions in which attackers have a correct node and range. It has a second network used for communicating with other attackers. The attacker generally cannot decrypt the encrypted data packet, and it does not know the correct location of the node. A set of attackers organised in a wormhole cannot continuously operate, neither in side-by-side locations nor at neighbouring nodes.

### *3.2 Problem Formulation*

In Fig. 1a, when nodes A and B, which are mobile nodes, come in contact, they will communicate. However, there is no confidence that risky neighbours may lie in that region. Though communication was protected by encryption, it is shown in Fig. 1c. Sometimes wormholes can communicate with nodes and affect the relay, causing a delay, so nodes will conduct MSND.

## 4 Proposed Method

An explanation of the MSND protocol's threat model is given in Fig. 1. Node A traverses a region. Figure 1a and b demonstrate that node B is likewise movable (b). Nodes strive to share data as they get closer to one another. Nevertheless, there is no guarantee that these possible neighbours genuinely live in the same neighbourhood via a wireless connection. Even if the contents of conversations between two nodes are protected by encryption, the nodes themselves might really be linked by a wormhole. A wormhole can selectively transmit, delay, or refuse messages, as seen in Fig. 1c, which is similar to the scenario described in Fig. 1a. The wormhole could trick Nodes A and B into believing they are neighbours when they are not. Nodes perform MSND to verify that the two communication channels are local to each other.

The principle of the MSND protocol is that as many nodes move, the length of the extension line is related to the distance between the nodes. The wormhole cannot interfere with different processes in a way that leads to the same action, because it does not know the distance between them all. The path to this perspective is through graphical rigidity.

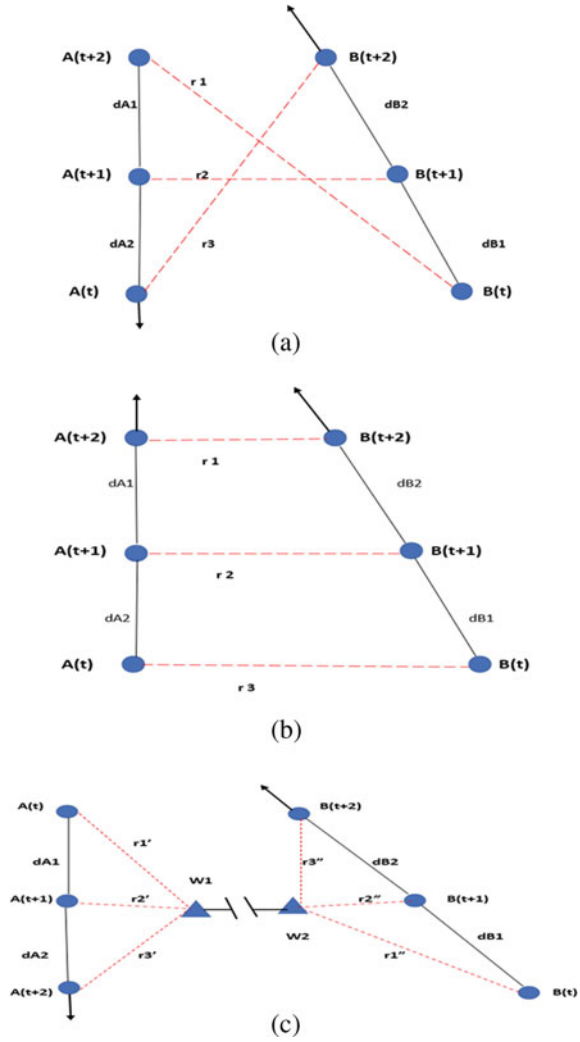


**Fig. 1** **a–c** MSND protocol framework

Laman's theorem in [8] states that a graph $G$ with rigid edges connected by flexible joints is solid in the plane if and only if it has $k$ vertices, independent $2k - 3$ sides, and a collection of more than $2k - 3$ corners.

In a sensor network, it is possible to explain how two nodes move along their pathways in relation to one another. The directions of movement may be parallel, convergent, or divergent. There are an infinite number of conceivable associations between the two range pathways in relation to one another. The directions of movement may be parallel, convergent, or divergent. There are an infinite number of conceivable associations between the two ranges. A stiff graph forms when there are four or more ranges, which restricts the number of relative pathways to a few distinct

cases. The predicted lengths of the following ranges may be precisely estimated in this stiff graph, and they can be contrasted with the ranged value itself.

The number of nodes and the number of wormholes are shown in (a) and (b) above. However, in the presence of a wormhole, the signal difference should propagate from the transmitter to the proximal side of the wormhole, along the wormhole, and then to the third and fourth nodes, as shown in Fig. 1c. If the difference between the nodes is the same, this difference is less noticeable with just two variables. But the movement changes the distance between each and the respective wormhole tip. This distance ($ri = r'\ i + r''i$, as shown in Fig. 1c) results in a larger-than-expected gap, and the line runs along a larger-than-expected difference over a long period of time.

In this section, we discuss the notation of variable consistency.

Though rigidity is an anticipated output in the movement of nodes, some cases affect the MSND protocol. In the first case, two nodes travelled in the same line as shown in Fig. 2a, and in the second case, nodes moved in parallel lines with the same ranging length.

**Algorithm 1: MSND Protocol**

1: NR do for $i = 1$

2: range $ri$ ←(node $A$, node $B$)

3: $dAi$, $dBi$ ← move(node $A$, node $B$)

4: end for

5: wh present ← Verification

6: if false = wh now then

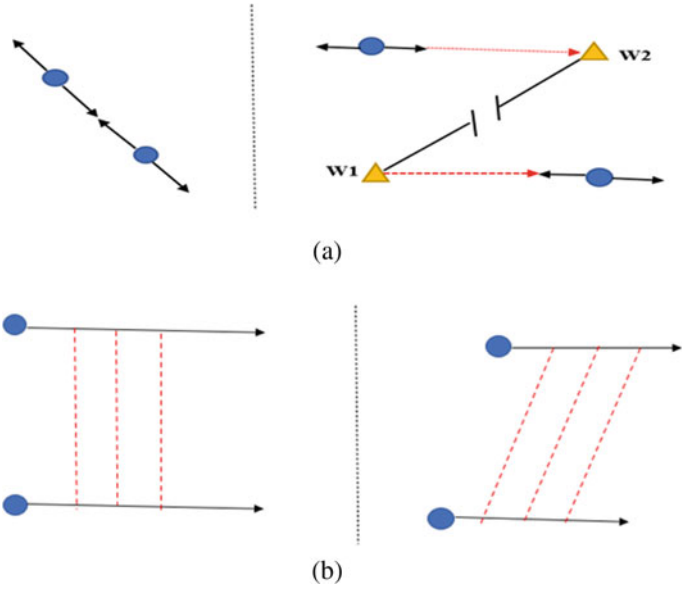


**Fig. 2** **a** All points collinear with wormhole. **b** All nodes are parallel with ranges are equal

7: neighbour
8: last if

From lines 1–4, node N–R ranging operations are executed, and from line 5, travel lengths and ranges are passed for verification. Here in this algorithm, *ri* represents the range between *A* and *b*, and *dAi* and *dBi* are variables used to assign values.

The MSND algorithm is chosen here to enhance efficiency and reliability of wireless sensor networks.

## *4.1 Ranging*

The range consists of three steps: synchronisation, transmission, and data exchange. In the synchronisation phase, node *A* sends the time-being packet encrypted with pairwise key *AB* and second packet pieces. Next, node *B* decrypts the time-being packet. Second phase of transmission in which node *A* sends the preamble packet to calculate the range. Node *B* calculates the time of receiving. Finally, there is the data exchange phase, in which node *A* sends the encrypted data packet with timing and distance $d_A$ and node *B* saves the data until the operations are done [9].

**Algorithm 2**
Verification
1: what to do now? ← Do a preliminary test
2: if (wh now) returns true
3: $i = 1$ to 3 for
4: Get $X \leftarrow$ solid graph $(D)$
5: $\tau \leftarrow$ Test fit $(X, y(x))$
6: Last
7: for wh now ← Voting ($\tau \geq$ TH or $\sigma \geq$ ST)
8: if (wh now and TestAngle)
9: if (angle $(X) \leq$ AT ) repeat warning
10: finish if
11: return if yes

Algorithm 2 is used to detect the distances and ranges travelled by nodes, or else it may be affected by wormholes if the two nodes are neighbours. Line 1 represents the preliminary checks; distance analysis is represented in Line 4, and output is in Line 7.

Here, the parameters TH (threshold value), AT (another threshold value), wh (wormhole and (standard deviation) are used in this algorithm.

## 5 Security Analysis

In this section we shown the security analysis of MSND.

**Preposition 1** *A wormhole, w1 to w2, cannot identify the range between two nodes in a sensor network.*

***Proof*** At different levels of MSND, the wormhole transmits different signals to other parties during transmission between sender and receiver. The receiver receives the signal. Although MSND needs to exchange RF packets, the transmission data is sorted, and the signal and reception are different [10].

**Preposition 2** *The wormholes w1 and w2 cannot find out the distance travelled by each mobile node.*

***Proof*** In the source node, the distance information accessible to the wormhole is meta data (a ranging signal). Ideally, the meta data related to the RF packet is available at the receiving node. It does not know about the speed of nodes in the transmission period, and meta data does not produce correct distance information.

**Preposition 3** *A wormhole (W1, W2), by reading the data packet when it is forwarded, cannot assume the distance ranges of nodes.*

***Proof*** A wormhole cannot break the encryption scheme using the system model [11].

**Theorem** *MSND is secure.*

***Proof*** Laman's theorem says that ideally, the graph $(V, E)$ is solid in the plane; it should have $n$ vertices and $2n - 3$ sides. A graph has more than $2n - 3$ edges that make up the subset $F \subseteq E$ satisfying both conditions. (1) $|F| = 2n - 3$ (2) $F' \subseteq F$, $F' = \emptyset$, $|F'| \leq 2k - 3$. In a rigid graph, the distance between the ranges is analysed only if the previous distance and ranges are already known. As stated in Preposition 1, the wormhole is unable to know the previous ranges travelled by nodes, delaying the signal transmission, which can affect the signal check. So the wormhole mitigates the delay. Even though Preposition 2 says that the wormhole cannot know the distance travelled by each node, the data is encrypted as per Preposition 3.

The lengths of $r2–r$ are unknown, and the lengths of the edges are also unknown because the wormhole does not know the edges.

## 6 Result and Discussion

In this experiment, simulation was conducted using Network Simulator Version 2. Tool command language (TCL) and C++ are the languages used for node movement and ranging. The node moved in a 900 × 300 area with a single wormhole. Node

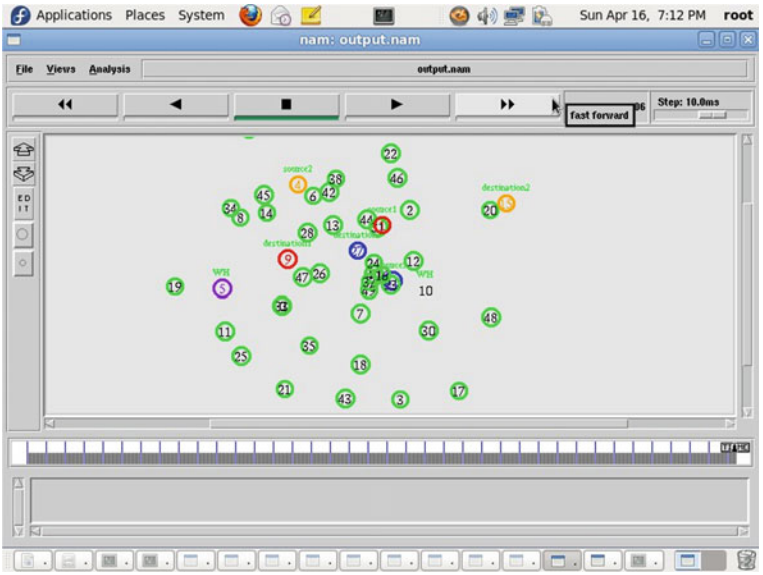


**Fig. 3** Output of wormhole attack

speed can be adjusted using NS2. The nodes do an analysis to confirm that two communicating nodes are local to the same neighbourhood. By examining 50 nodes in the network simulator software, we were able to evaluate the wireless sensor node in this project and discover the wormhole. This node's 12 and 13 are configured as the source and destination nodes, and 14 and 15 are identified as wormholes by code.

In this paper, we're utilising the MSND protocol, which can deliver a packet even when a wormhole is present while detecting the distance between neighbouring nodes. False positive ratio is the metric used if a wormhole is present, and true negative ratio is the metric that represents wrongly even if a wormhole is present. Output of wormhole attack is shown in Fig. 3.

### I. Throughput

Throughput is the amount of data packet delivered within given time. In our project using MSND protocol delivery of data is high when compared with sectoral form it is shown on graph (Fig. 4).

### II. Packet Delivery Ratio (PDR)

Packet delivery ratio: the ratio at which calculated data packets are delivered to destinations from the source node. According to the graph, *Ri*/*Si* calculated it, and the MSND protocol probably places it high (Fig. 5).

### III. Detection Ratio

The ratio at which it detects its neighbour node for sending data packet the detection ratio is higher when compared with sector form (Fig. 6).

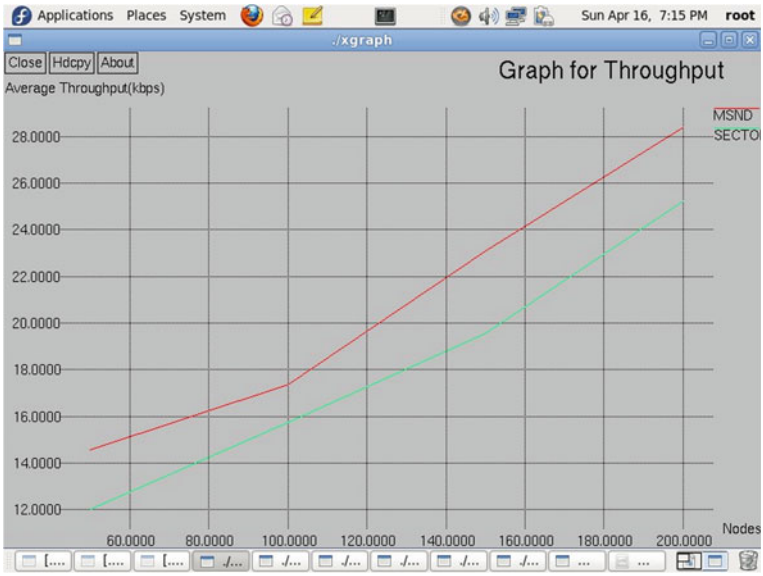


**Fig. 4** Throughput

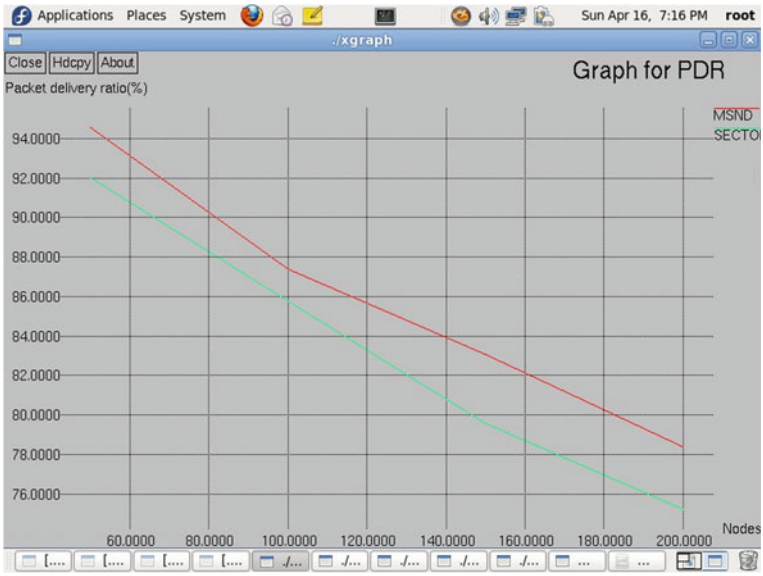


**Fig. 5** Packet delivery ratio

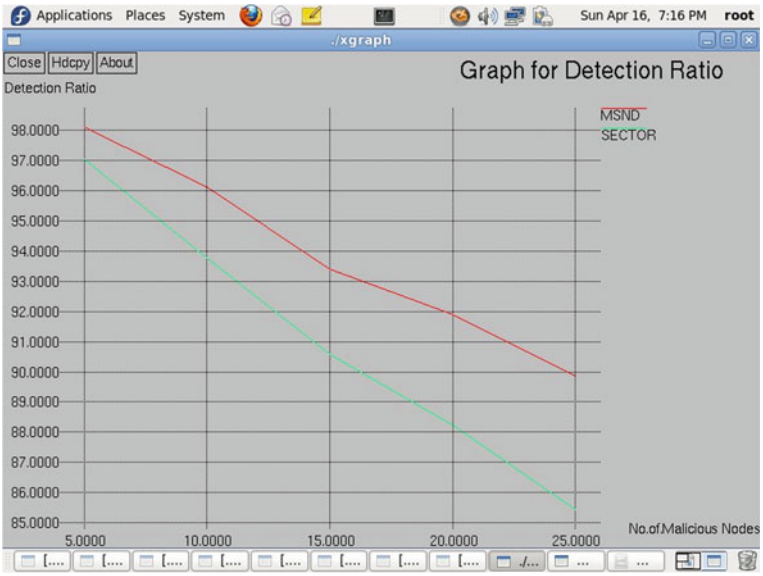


**Fig. 6** Detection ratio

## IV. Energy

Energy needed for packet transmission when compared with sector it needs less energy. It is shown on Fig. 7.

## V. Packet Loss

Packet loss (Fig. 8) is the amount of data packet wormhole swallowed; the packet ratio must be less in the MSND protocol.

## VI. Overhead

Overhead (Fig. 9) tells how much routing and control information is needed for the application data to reach the destination node. In our project, less is shown on the graph.

## VII. Average Delay

The overall delay is the amount of time the source sent packets are lost due to wormholes when we try to recover the delay that occurred for packet reception. It is calculated by dividing the total delay by the count. Average delay is shown in Fig. 10.

## VIII. True Negative Ratio

The true negative ratio is also called specificity; it is the actual negative rate as test negative and is calculated as TN/TN + FP. Using the MSND protocol, true negative ratio detecting capacity is high. Average delay is shown in Fig. 11.

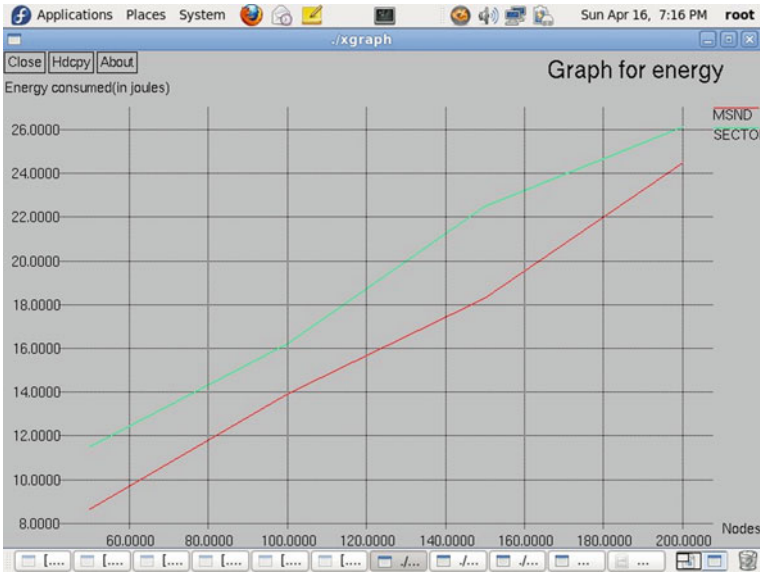


**Fig. 7** Energy

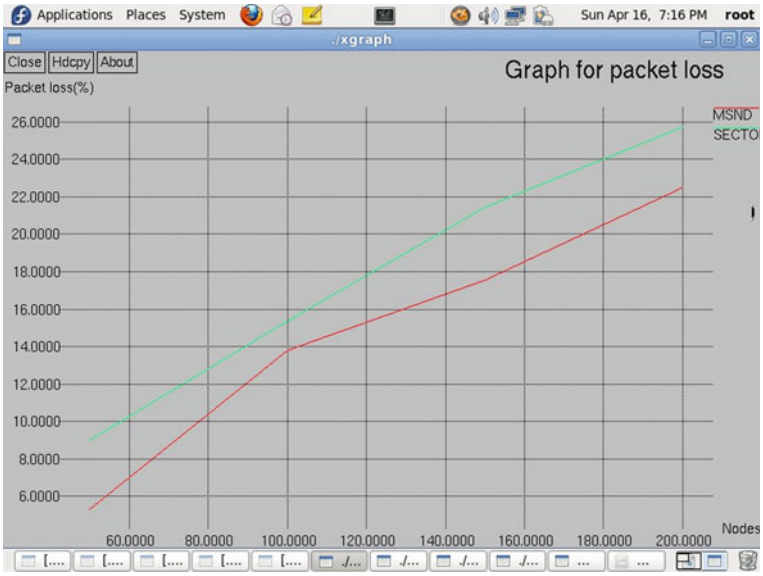


**Fig. 8** Packet loss

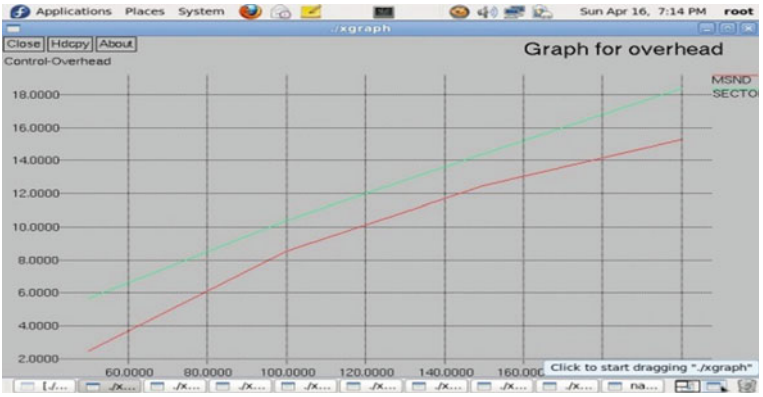


**Fig. 9** Overhead

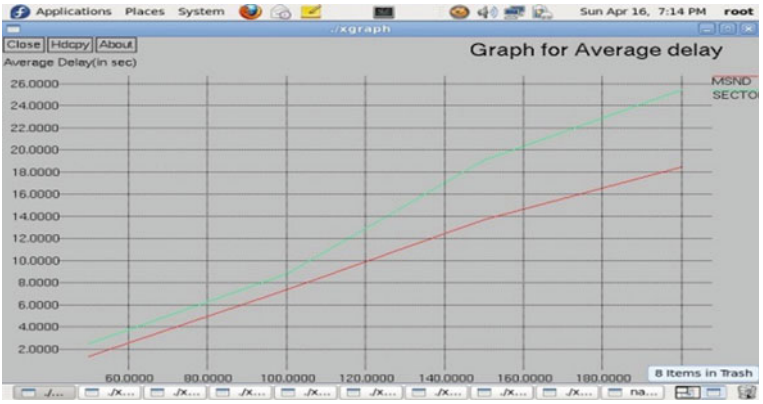


**Fig. 10** Average delay

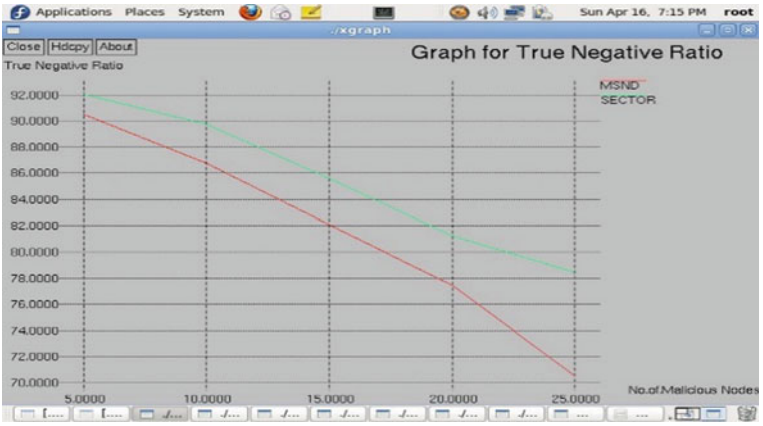


**Fig. 11** Average delay

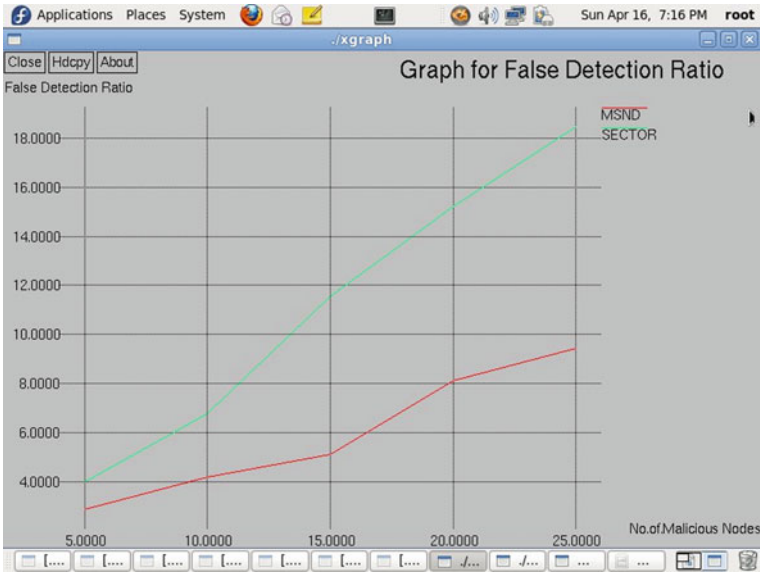


**Fig. 12** False detection ratio

### IX. **False Detection Ratio**

False detection ratio (Fig. 12) is the number of false nodes (wormhole) is detected using MSND in our project its accuracy ratio is high.

## 7 Conclusion

In this paper, a Mobile Secure Neighbour Discovery Protocol (MSND) is proposed to prevent the wormhole attack in wireless sensor networks. MSND ensures the secure and efficient discovery of neighbour nodes, which is a fundamental task in WSNs. The proposed protocol utilised the mobility of sensor nodes and the concept of trust management to discover neighbours securely and efficiently. The simulation results demonstrated that the proposed protocol outperformed the existing protocols in terms of network lifetime, energy consumption, and detection accuracy of wormhole attacks.

## References


1. Luo X, Chen Y, Li M, Luo Q, Xue K, Liu S, Chen L (2019) CREDND: a novel secure neighbour discovery algorithm for wormhole attack. IEEE Access 7:18194–18205
2. Priyantha NB, Chakraborty A, Balakrishnan H (2000) The cricket location-support system. In: Conference on mobile computing and networking (Mobicom)
3. Hu Y, Perrig A, Johnson D (2003) Packet leashes: a defense against wormhole attacks in wireless networks. In: International conference on computer communications (Infocom)
4. Xu Y, Ouyang Y, Le Z, Ford J, Makedon F (2007) Analysis of range-free anchor-free localization in a WSN under wormhole attack. In: ACM international conference on modeling, analysis and simulation of wireless and mobile systems (MSWiM)
5. Ho J-W, Wright M (2017) Distributed detection of sensor worms using sequential analysis and remote software attestations. IEEE Access 5:680–695
6. Luo Q, Wang J (2018) FRUDP: a reliable data transport protocol for aeronautical ad hoc networks. IEEE J Sel Areas Commun 36(2):257–267
7. Wang J, Liu Y, Niu S, Song H, Jing W, Yuan J (2021) Blockchain enabled verification for cellular-connected unmanned aircraft system networking. Future Gener Comput Syst 123:233–244. https://doi.org/10.1016/j.future.2021.05.002
8. Ditzel M, Langendoen K (2005) D3: data-centric data dissemination in wireless sensor networks. In: Proceedings of European conference on wireless technologies, Paris, France, pp 185–188
9. Asha G, Santhosh R (2019) Soft computing and trust-based Self-organised hierarchical energy balance routing protocol (TSHEB) in wireless sensor networks. Soft Comput 23(8):2537–2543
10. Aliady WA, Al-Ahmadi SA (2019) Energy preserving secure measure against wormhole attack in wireless sensor networks. IEEE Access 7:84132–84141
11. Yang Y, Wang H, Zhang J, Guizani M (2022) A secure and efficient neighbor discovery protocol for wireless sensor networks. IEEE Internet Things J 9(3)