AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Wormhole Attack Detection Algorithm Using Near Field Communication

[1]G. Vaishnav and [2]Dr. R. Dhaya

[1]*M.E. Computer Science and Engineering Velammal Engineering College, India.*
[2]*Associate Professor, Department of Computer Science and Engineering, India.*

Address For Correspondence:
G. Vaishnav, M.E. Computer Science and Engineering Velammal Engineering College, India.
E-mail: vaishu.gg@gmail.com

ARTICLE INFO

Article history:
Received 12 February 2016
Accepted 12 March 2016
Available online 20 March 2016

Keywords:
Distributed Algorithm, Near Field Communication (NFC), network security, wireless sensor network, Wormhole attack.

ABSTRACT

In wireless sensor network to improve the system performance, network coding is an effective approach. In contrast to traditional approach, in wireless network coding systems, the forwarders are allowed to apply encoding schemes on what they receive, and thus they create and transmit new packets. In a wormhole attack, the attacker can forward each packet using wormhole links and without modifying the packet transmission by routing it to an unauthorized remote node. Hence, receiving the rebroadcast packets by the attackers, some nodes will have the illusion that they are close to the attacker. With the ability of changing network topologies and bypassing packets for further manipulation, wormhole attackers pose a severe threat to many functions in the network, such as routing and localization. To overcome this vulnerability issue, we use a centralized algorithm and a distributed detection algorithm, DAWN against wormhole, partnering with ETX and Near Field Communication (NFC). In this paper, we mainly focus on how much the detection capacity is efficient when we use NFC tags with sensor nodes, as they provide authenticity through unique identification.

INTRODUCTION

A wireless sensor network (WSN) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity.Since this network is infrastructure-less, they are exposed to many threats like Spoofed, altered, or replayed routing Information, Selective forwarding, Sinkhole attacks, Sybil attacks, Wormholes, HELLO flood attacks and so on. In all the above attack, this paper is going to concentrate on wormholes which cause serious threat to the system integrity.Wormhole attack is a devastating attack where two malicious colluding sensor nodes create a virtual tunnel in the wireless sensor network, which is used to forward message packets between the tunnel edge points the analysis of inevitable symptom wormhole in the network without using any special hardware and develop a distributed detection with some restriction. An adversary is an outsider, who does not have a valid network identity and also not a part of the network. The attackers have the capability to launch a variety of attacks, such as dropping or corrupting the relayed packets, that significantly harms a lot of network protocols including energy efficient routing, localization, and etc. The basic severe feature of wormhole attack lies in the fact that the attackers can easily launch a virtual wormhole without understanding the protocols or cryptographic mechanisms used in the network. The Fig. 1 below is the pictorial representation of wormhole in sensor network.

To Cite This Article: G. Vaishnav and Dr. R. Dhaya., Wormhole Attack Detection Algorithm Using Near Field Communication. ***Aust. J. Basic & Appl. Sci.,*** *10(1): 517-523, 2016*

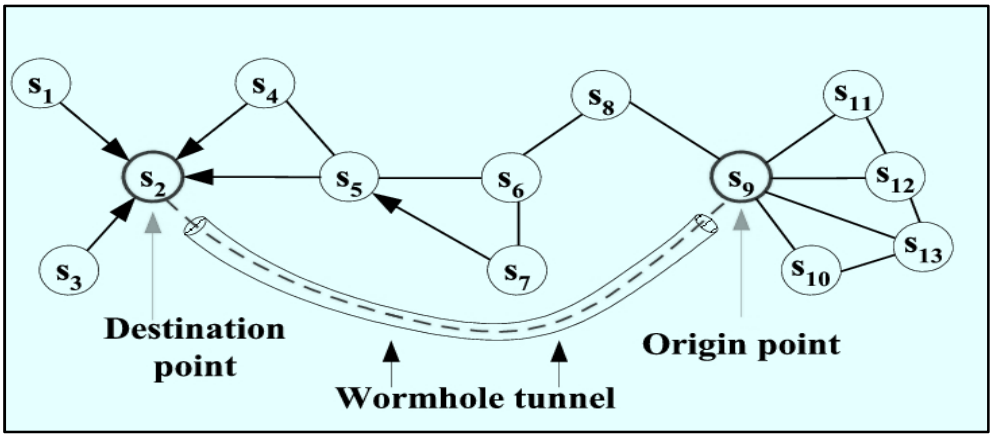

Fig. 1: representation of wormhole

In the efforts made to enhance the system performance, network coding system constitutes a different approach which is effective than traditional networking approach. In random linear network coding approach, the intermediate nodes store and forward the encapsulated packets which are de-capsulated at the destination node to find the message similar to the original message. Here the message on transmission to neighbouring nodes, the forwarding nodes are allowed to apply encoding schemes on packets they receive, hence transmitting a new packet. This type of encoding technique significantly enhances the system performance. With reference to wormhole attack, many contributions were made before. In-spite of that, many attacks are prevalent as all the present mechanism fail to take preventive measures for wormholes. Thus this paper takes a forward step to prevent the wireless sensor network from wormholes. In this paper, we have reviewed the various related works on wormhole attack algorithms in the second section. In section III, we have the proposed system. The simulation setup in section IV and the comparison of system attributes after and before encapsulating NFC in WSN in the following section.

II. Related works:

Recently, many attentions are made towards the wormhole attack algorithm. Different attributes are taken into account and many algorithms were proposed to identify and detect wormhole attack in wireless network system. According to this, for detection of wormhole attacks in WSN, algorithms based on various attributes are used such as follows are used.

- Location based end to end detection
- Using graph structure
- Time based approach
- Link state routing approach
- Identity based approach
- Linear programming model

All the algorithms follow various drawbacks according to their situation and are summarized in the table below.

Table 1: Summarized approaches and limitations

S. No	APPROACH	ATTRIBUTES TAKEN CARE	LIMITATIONS
1	Location based end to end detection (Wei, Y. and Y. Guan, 2013; Wang, Y., Z. Zhang and J. Wu, 2010)	Sensor location, hop count	Irresistible packet loss when attacker is hidden and the chances of false alarm is high
2	Detection using graph structure (Maheshwari, R., *et al*., 2017)	Connectivity information with shortest path algorithm in graph structure	Maintenance of graph structure for mobile nodes are difficult and any nodes can cluster with the cluster head
3	Time based approach (Kim, J., *et al*., 2010; Zhao, Z., *et al*., 2010; Prasannajit, B., *et al*., 2010)	Time synchronization and delay in hop with respect to Round trip time	False alarm is produced when bulky data is sent.
4	Link state routing approach (Attir, A., *et al*., 2007)	WP- OLSR algorithm, table maintained for sent and received HELLO message.	Since the table must be distributed among all nodes after each update, the power consumption will be more also it is vulnerable to attack.

5	Identity based approach (McAuley, A., *et al*., 2006)	Co- operative intrusion detection Algorithm	When the cluster grows, then the node identity structure also grows complex
6	Linear Programming Model (Vaishnavi, G. and R. Dhaya, 2015; Vaishnavi, G. and R. Dhaya, 2015)	Distributed algorithms and ETX (expected transmission count)	This approach even serves better when unique node identification is provided.

All the above approach requires either to use an established route that does not exist with network coding, or to calculate the delay between every two neighbouring nodes. This introduces a huge amount of errors in the network.

III. Proposed sysyem:

In this paper we have proposed a wormhole detection technique by incorporating another technology called Near Field Communication with the existing network constraints. This NFC tags are normally used for end to end data transfer in mobiles (Vaishnavi, G. and R. Dhaya, 2015). But we have made a forward step to use this unique ID of NFC tags to enhance the security feature of Wireless Sensor Network. To elaborate about NFC, it is a kind of wireless communication technology built upon the existing Radio-Frequency Identification (RFID) standards.For example, NTAG213 or NTAG216 both have a read/write password built-in support. Also they use Unique ID of the tag, which cannot be duplicated, as a part of Hash/Encryption/Check/Salt so it can only be decrypted by the same tag ID it was copied from. Hence, by using NFC tags in wireless nodes we can create a secure environment for communication free from wormholes. Even-though the wormholes are detected through algorithms proposed in (Ji, S., *et al*., 2005), we incorporate NFC in the existing approach to set up a network with reduced loss and delay by achieving maximum reliability and throughput.

IV. Simulation setup:

To evaluate the efficiency of DAWN proposed in and the incorporation of NFC in that, we have used NS2 network simulator version 2.35. We have created 25 nodes which uses Random Linear Network Coding(RLNC) for communication. With the help of this setup, various algorithms are implemented and their outcomes are visualised.

4.1. Node creation and network formation:

As specified earlier, we have created 25 nodes which communicate through Random Linear Network Coding (RLNC) scheme. The use of limited number of nodes is to study the detection of wormholes clearly within a cluster of WSN.The initial setup in simulator is shown in the Fig. 2 below.

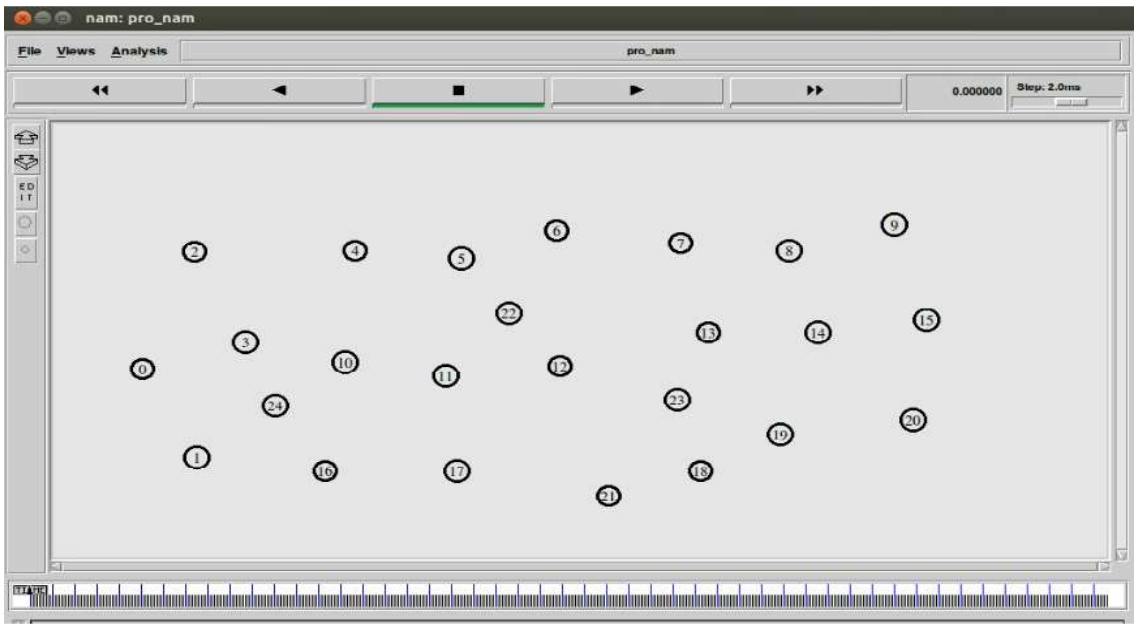

Fig. 2: Initial setup

4.2. Wormhole detection:

First the source node and the destination nodes are set. Then a path is laid between the source and destination by multi hops. This multi hops are made through the nearest neighbour. In that path, a particular node is selected as adversary node which finds its clone node. This adversary node is selected in such a way where more number of neighbouring nodes is present. This clone node, gathers the information of all the neighbouring nodes. Hence, it can be easily influenced by the attacker node and these nodes are considered malicious. This clone is not only malicious, also it is considered as one mouth of the wormhole, which has its pair either in different cluster or in same cluster (if the cluster capacity is high in both number and range of access). The Fig. 3 shows the adversary and clone node and the Fig. 4 shows the neighbourhood information collected by the clone node.

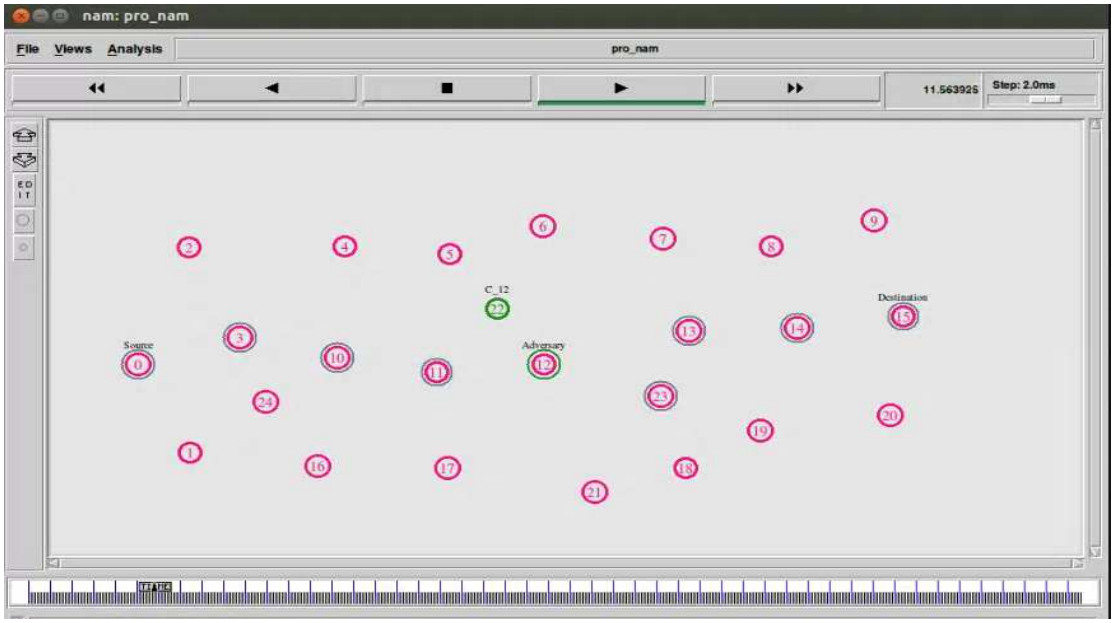

Fig. 3: Adversary and clone node

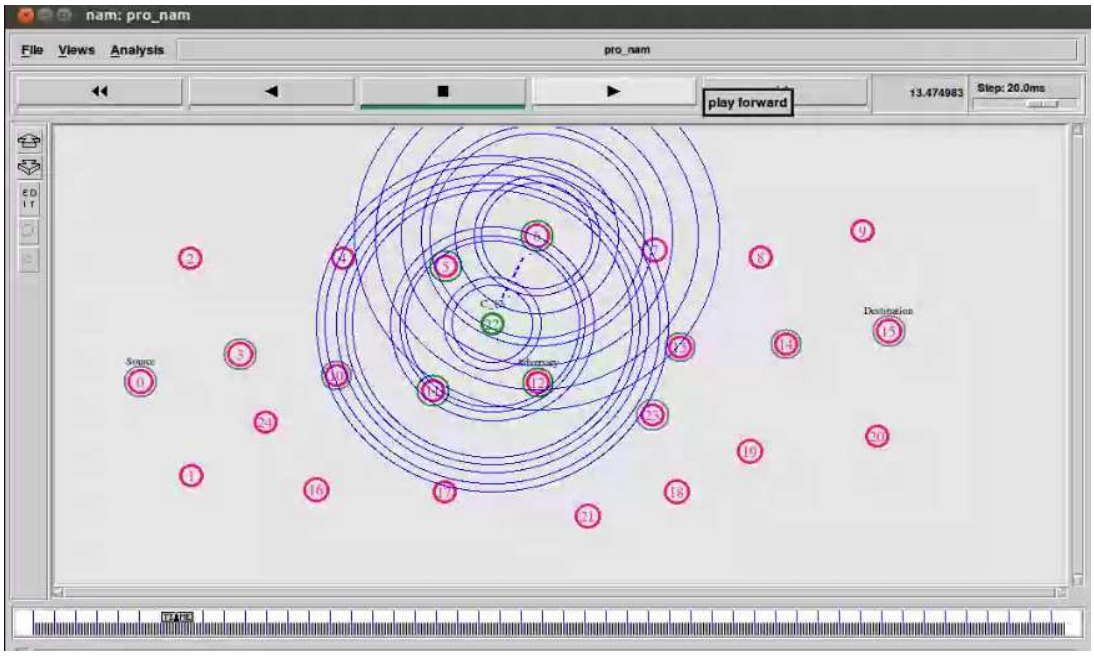

Fig. 4: information collection by the clone node from the neighbour

4.3. Role of NFC:

After all the clone node is found, the information about the clone is routed to all the nodes in the network. After this, any transmission made, the other nodes boycott the clone node. To overcome the adverse effect, we have proposed a method in this paper as follows.After detecting the clones in the cluster, the cluster is split into different zones with their own zone source and zone destination as shown in the Fig. 5. Now, for all the nodes in all zones, NFC tag is set with their own ID (unique ID). So, when the source forwards the packet to its neighbour, it collects all the NFC IDs of its zone. If the communication is inter-zone transmission, the NFC IDs of that zone is also collected by the forwarding node. Hence, even if such clones are present, the nodes can transmit the packet confidently through clones without bothering about the attacker nodes.

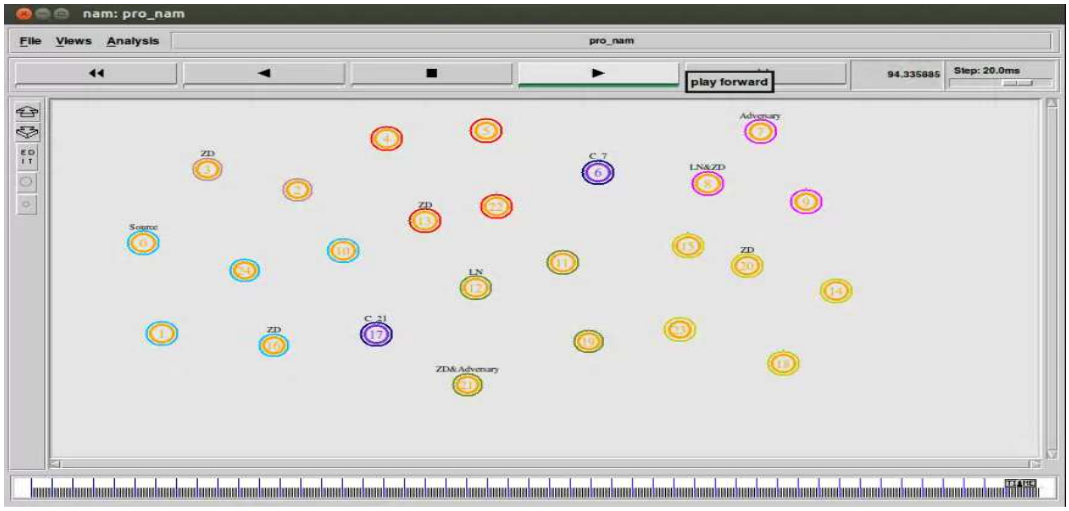

Fig. 5: classification of zones

In this construct, it should be ensured by the forwarding node that the node which is going to receive the packet has NFC ID and it is present in one of the zones of the cluster.

V. Comparison of system attributes:

5.1. Packet loss:

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Here the packet loss in the WSN is evaluated during both before and after incorporation of NFC. It is clearly viewed that the packet loss is reduced while using NFC and hence the reliability is improved.

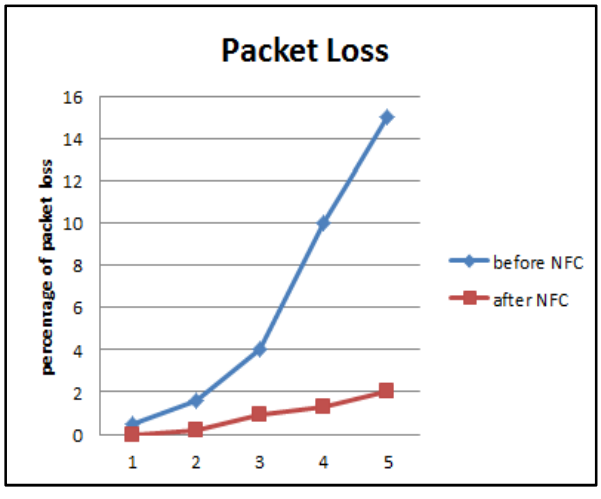

Fig. 6: percentage of packet loss before and after using NFC

5.2. Throughput:

Throughput is the rate of successful message delivery over a communication channel. It is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot. Here, the difference in throughput obtained on incorporating NFC is specified.

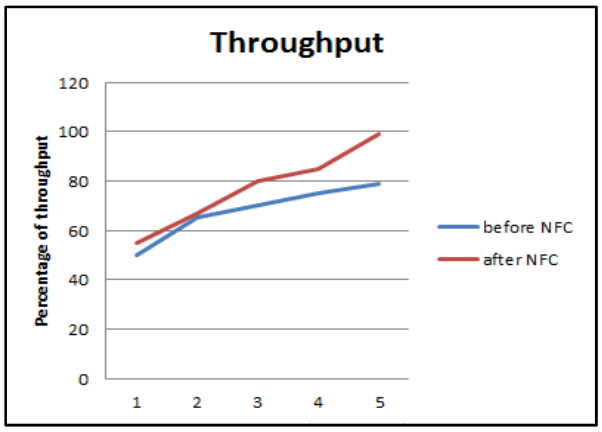

Fig. 7: percentage of throughput before and after using NFC

5.3. Delay:

The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. The Fig. 8 specifies the delay occurred in the WSN during both before and after using NFC and are compared.

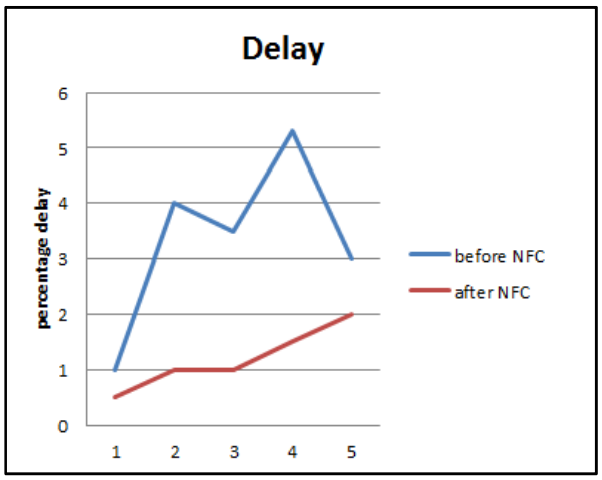

Fig. 8: percentage of delay occurred before and after using NFC

Conclusion:

In this paper we have investigated the wormhole detection algorithms and a deep study is made on the adversary model of wormhole detection in WSN using a simulation setup. Here we have also proposed a new methodology to improve the authentication of the nodes in the network through Near Field Communication (NFC). The study made on various performance metrics, prove that this method is efficient in enhancing both reliability and throughput.

REFERENCES

Attir, A., F. Naït-Abdesselam, B. Bensaou and J. Ben-Othman, 2007. Logical wormhole prevention in optimized link state routing protocol. In *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE* pp: 1011-1016.

Ji, S., T. Chen and S. Zhong, 2015. Wormhole attack detection algorithms in wireless network coding systems. Mobile Computing, IEEE Transactions on, 14(3): 660-674.

Kim, J., D. Sterne, R. Hardy, R.K. Thomas and L. Tong, 2010. Timing-based localization of in-band wormhole tunnels in MANETs. In *Proceedings of the third ACM conference on Wireless network security* (pp. 1-12). ACM.

Maheshwari, R., J. Gao and S.R. Das, 2007. Detecting wormhole attacks in wireless networks using connectivity information. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE* (pp. 107-115). IEEE.

McAuley, A., K. Manousakis, D. Sterne, R. Gopaul and P. Kruus, 2006. Creating and maintaining a good intrusion detection hierarchy in dynamic ad hoc networks. In *Military Communications Conference, 2006. MILCOM 2006. IEEE* (pp. 1-6). IEEE.

Prasannajit, B., S. Anupama, K. Vindhykumari, S.R. Subhashini and G. Vinitha, 2010. An approach towards detection of wormhole attack in sensor networks. In Integrated Intelligent Computing (ICIIC), 2010 First International Conference on pp: 283-289.

Vaishnavi, G. and R. Dhaya, 2015. A Survey on Wormhole Attack Detection Algorithm. International Journal, 3(11): 597-602.

Vaishnavi, G. and R. Dhaya, 2015. A Survey on Wormhole Attack Detection Algorithm. International Journal, 3(11): 597-602.

Vaishnavi, G. and R. Dhaya, 2015. A Survey on Wormhole Attack Detection Algorithm. International Journal, 3(11): 597-602.

Wang, Y., Z. Zhang and J. Wu, 2010. A distributed approach for hidden wormhole detection with neighborhood information. In *Networking, Architecture and Storage (NAS), 2010 IEEE Fifth International Conference on* (pp. 63-72). IEEE.

Wei, Y. and Y. Guan, 201). Lightweight location verification algorithms for wireless sensor networks. Parallel and Distributed Systems, IEEE Transactions on, 24(5): 938-950.

Zhao, Z., B. Wei, X. Dong, L. Yao and F. Gao, 2010. Detecting wormhole attacks in wireless sensor networks with statistical analysis. In *Information Engineering (ICIE), 2010 WASE International Conference on* 1: 251-254.