A SURVEY ON SECURITY ISSUES TO DETECT WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK

Priya Maidamwar[1] and Nekita Chavhan[2]

[1]Wireless Communication & Computing, Department of Computer Science & Engineering, G H. Raisoni College of Engineering, Nagpur, India
priyamaidamwar2189@gmail.com
[2] Computing, Department of Computer Science & Engineering, G. H. Raisoni College of Engineering, Nagpur, India
niki.chavan@gmail.com

ABSTRACT

Sensor nodes, when deployed to form Wireless sensor network operating under control of central authority i.e. Base station are capable of exhibiting interesting applications due to their ability to be deployed ubiquitously in hostile & pervasive environments. But due to same reason security is becoming a major concern for these networks. Wireless sensor networks are vulnerable against various types of external and internal attacks being limited by computation resources, smaller memory capacity, limited battery life, processing power & lack of tamper resistant packaging. This survey paper is an attempt to analyze threats to Wireless sensor networks and to report various research efforts in studying variety of routing attacks which target the network layer. Particularly devastating attack is Wormhole attack- a Denial of Service attack, where attackers create a low-latency link between two points in the network. With focus on survey of existing methods of detecting Wormhole attacks, researchers are in process to identify and demarcate the key research challenges for detection of Wormhole attacks in network layer.

KEYWORDS

Denial of Service, Mobile adhoc network, Security, Wireless sensor network, Wormhole attacks.

1. INTRODUCTION

Wireless sensor networks as a part of MANET consists of a large number of tiny sensor nodes that continuously monitors environmental conditions. Sensor nodes perform various significant tasks as signal processing, computation, and network self-configuration to expand network coverage and strengthen its scalability. The sensors all together provide global scenario of the environments that offer more information than those provided by independently operating sensors. They are also responsible for sensing environment and transmission information. Usually the transmission task is critical as there is huge amount of data and sensors devices are restricted. As sensor devices are limited the network is exposed to variety of attacks. Traditional security mechanisms are not applicable for WSNs as they are usually heavy and nodes are limited. Also these mechanisms do not eliminate risk of other attacks. WSNs are useful in various critical domains such as environment, industry, military, healthcare, security and many others. For an instance, in a military operation, a wireless sensor network monitors several activities. If an event is detected, these sensor nodes sense it and report the information to the base station (called sink)

by communicating with other nodes. To collect data from WSNs, base stations are generally used. They usually have more resources (e.g. computation power and energy) than normal sensor nodes which have more or less such constraints. Aggregation points gather data from neighbouring sensor nodes integrate the data and forward them to base stations, where the data are further processed or forwarded to a processing centre. In this way, energy can be conserved in WSNs and network life time is thus prolonged.

WSNs have some special characteristics that distinguish them from other networks such as MANET. The characteristics, are listed as follows, that can lead to the use of WSNs in the real world:

• Sensor nodes possess extremely limited resources, such as battery life, memory space and processing capability. Routing protocols and algorithms are preferred to achieve longer sensor life.

• WSNs are self configuring and self organizing wireless networks.

• The topology of sensor network changes rapidly and randomly. Sensor nodes are continuously added and deleted from the network.

• WSNs have centralized approach in terms of network control. Data flows from sensor nodes towards a few aggregation points which further forward the data to base stations. Also base stations could broadcast query/control information to sensor nodes [1].

Among the designs of WSNs, security is one of the significant aspects that deserve great attention, considering the tremendous application opportunities. Thus keeping in mind security constraints this paper presents a brief review of existing techniques for wormhole attack detection in network layer.

Thus, the survey paper focuses on various approaches to detect wormhole attacks. Section 2 describes the challenges of sensor networks; section 3 presents attacks on sensor networks; section 4 studies background and significance of wormhole attack; section 5 describes wormhole attack model; section 6 presents types of wormhole attack; section 7 describes countermeasures to wormhole attacks and section 8 followed by future research challenges. Section 9 describes the conclusion.

2. CHALLENGES OF SENSOR NETWORKS

A wireless sensor network is a special network which has many constraint compared to a conventional computer network Security in wireless sensor networks has attracted a lot of attention in the recent years. Majority of resource constraints makes computer security more challenging task for these systems. The various challenges are discussed as follows.

.

2.1. Wireless nature of communication

The open nature of wireless medium is inherently less secure and thus makes it vulnerable against various kinds of malicious attacks. These attacks can be either passive or active attacks. Passive attack intends to steal information and to eavesdrop on communication within the network In active attacks, attacker modifies and injects packets into the network. This factor should be taken into consideration so that performance of the system is not significantly affected.

2.2. Ad-Hoc Deployment

Sensor nodes are deployed randomly and do not have any fixed topology. The ad-hoc nature of sensor networks means no regular structure can be defined. Due to high mobility of nodes network topology is always subject to changes. Hence security mechanisms must be able to operate within this dynamic environment.

2.3. Hostile Environment

Hostile environment in which sensor nodes are deployed is another challenging factor. Due to the broadcast nature of the transmission medium, wireless sensor networks are vulnerable to various security attacks. Moreover nodes are placed in a dangerous or unguarded environment where they are not physically protected. Attackers may capture a node, physically tamper it, and extract valuable information from it. The highly hostile environment represents challenging approach for security researchers.

2.4. Resource Limitation

Adequate amount of resources are mandatory for the implementation of all security approaches. including memory, bandwidth, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor which poses considerable challenges to resource-hungry security mechanisms.

2.4.1 Limited Memory and Storage Capacity:

Sensor node is a tiny device with very small amount of memory and storage space for the code. It is necessary to limit the code size of the security algorithm in order to develop an effective security mechanism.

2.4.2 Power Limitation:

The use of wireless sensor networks is increasing day by day and since each node depends on energy for its activities, this has become a biggest constraint and primary requirement in wireless sensor networks. The failure of one node can destroy the entire system. Therefore, some mechanisms must be designed to conserve energy resource.

2.5. Scalability

Scalability is a major factor in wireless sensor networks. A network topology is dynamic, it changes depending upon the user requirements. All the nodes in the network area must be scalable so as to adapt themselves with changing network topology.

2.6. Unreliable Communication

Certainly, unreliable nature of communication channel is another challenging issue to sensor security. The security of the network depends heavily on a defined protocol, which in turn depends on communication.

2.6.1 Unreliable Transmission:

Sensor network follows packet-based routing approach for communication. Hence transmission is connectionless and therefore inherently unreliable.

2.6.2 Conflicts:

Although the channel is reliable, the communication may still be unreliable because of congestion of data packets. This is due to the broadcast nature of the wireless sensor network.

2.6.3 Latency:

Latency is defined by how much time a node takes to monitor, or sense and communicate the activity. Sensor nodes gather information, process it and send it to the base station. Latency in a network is computed based on these activities as well as how much time a sensor node takes to forward the data in heavy network traffic or in a low density network.

2.7. Unattended Operation

In certain cases, the sensor nodes are not operated and hence are left unattended for long periods of time. There are three main reasons to unattended sensor nodes.

2.7.1 High risk of Physical Attacks:

After deployment, sensors are usually left unattended and easy to be physically compromised. An adversary can capture one or more nodes, injects some malicious code into them to cause threats or receives information from the network. Also, an adversary can easily eaves drop the transmission or launch serious attacks. Therefore, it is not surprising that sensor networks are vulnerable to many security attacks.

2.7.2 Managed Remotely:

Remote management of a sensor network makes it difficult to detect physical tampering and physical maintenance issues.

2.7.3 Lack of Central Coordinator:

A sensor network should be a distributed network. Each sensor node should operate autonomously with no central point of control in the network. In case if designed inaccurately, it will make the network organization difficult, inefficient, and weak. A sensor node left unattended for longer time is more likely to be compromised by an adversary [2].

3. ATTACKS ON WIRELESS SENSOR NETWORKS

Wireless sensor networks are susceptible to wide range of security attacks due to the multi-hop nature of the transmission medium. Also, wireless sensor networks have an additional vulnerability because nodes are generally deployed in a hostile or unprotected environment. Although there is no standard layered architecture of the communication protocol for wireless sensor network, hence there is need to summarize the possible attacks and security solution in different layers with respect to ISO-OSI model as follows[3]:

Table 1. Layering based attacks and possible Security approaches

Layer	Attacks	Security approaches
Physical Layer	Denial of Service Tampering	Priority Messages Tamper Proofing Hiding, Encryption [4].
Data Link Layer	Jamming Collision Traffic manipulation	Use Error Correcting Codes Use spread spectrum techniques
Network Layer	Sybil attack Wormhole attack Sinkhole Flooding	Authentication Authorization Identity certificates
Transport Layer	Resynchronization Packet injection attack	Packet Authentication
Application Layer	Aggregation based attacks Attacks on reliability	Cryptographic approach

3.1. Definitions, Strategies and Effects of Network Layer Attacks on WSN

WSNs are organized in layered form. This layered architecture makes these networks vulnerable and lead to damage against various kinds of attacks. For each layer, various attacks and their defensive mechanisms are defined. Thus, WSNs are vulnerable to different network layer attacks, such as black hole, gray hole, wormhole, sinkhole, selective forwarding, hello flood, acknowledgement spoofing, false routing, packet replication and other attacks to network layer protocols [3].

Now, the following table shows network layer attacks on WSNs, its classification and comparison based on their strategies and effects.

Table 2. Classification of Network layer attacks on WSN

Attack/Criteria	Attack Definition	Attack Effects
Black hole	In a black hole attack, the attacker swallows (i.e. receives but does not forward) all the messages he receives, just as a black hole absorbing everything passing by.	• It can disrupt the communication between the base station and the rest of the WSN, and hence prevent the WSN from serving its purposes. • Throughput of a subset of nodes, around the attacker and with traffic through it, is decreased [1].
Wormhole	A wormhole attack requires two or more adversaries. These adversaries have better communication resources (e.g. power, memory) than normal nodes, and can establish better communication channels (called "tunnels") between them [1].	• False/forged routing information. • Change the network topology. • Packet destruction/alteration by wormhole nodes. • Changing normal messages stream.
Sybil	In Sybil attack, a malicious node attracts network traffic by representing multiple identities to the network [6].	• Confusion and WSN disruption. • Enable other attacks. • Exploiting the routing race conditions.
Sinkhole	Sinkhole is a more complex attack compared with black hole attack [1].	• Attracts almost all the traffic. • Triggering other attacks, such as eavesdropping, trivial selective forwarding, black hole and wormhole. • Changes the base station's position.
Selective forwarding	In Selective forwarding attack, attacker refuses to forward packets or selectively drop them and act as a black hole [7].	• Message modification. • Information fabrication and packet dropping. • Suppressed messages in a certain area. • Routing information modification. • Exhaustion of resources
Hello flood	In Hello Flood Attack, attacker broadcast hello message with strong transmission power to the networks and acts as a fake sink [7].	• Creates an illusion to base station of being a neighbor to many nodes in the networks. • Confuse the network routing badly.[2]
Acknowledgement Spoofing	An adversary can spoof Network layer acknowledgements (ACKs) of overheard packets	• False view/information of the WSN. • Launch selective forwarding attack. • Packet loss/corruption.
False Routing(Misdirection Attack)	Attacker routes the packets to false destination, creates the loops in networks [8].	• False and misleading messages generated; • Resources exhaustion; • Degrade the WSN Performance

4. BACKGROUND AND SIGNIFICANCE OF WORMHOLE ATTACK

Scarcity of various resources makes wireless sensor network vulnerable to several kinds of security attacks. Attacker possessing sufficiently large amount of memory space, power supply, processing abilities and capacity for high power radio transmission, results in generation of several malicious attacks in the network. Wormhole attack is a type of Denial of Service attack that misleads routing operations even without the knowledge of the encryptions methods unlike

other kinds of attacks. This characteristic makes it very important to identify and to defend against it [9].

Wormhole attack is a severe type of attack on Wireless sensor network routing where two or more attackers are connected by high speed off-channel link called wormhole link [10].

Wormhole attacks exists in two different modes, namely 'hidden' and 'exposed' mode, depending on whether attackers put their identity into packet headers when tunnelling and replaying packets [11].

In wormhole attack, a pair of attackers forms 'tunnels' to transfer the data packets and replays them into the network. This attack has a tremendous effect on wireless networks, especially against routing protocols. Routing mechanisms can be confused and disrupted when routing control messages are tunnelled. The tunnel formed between the two colluding attackers is referred as wormhole. Figure 1 shows the wormhole attack. Packets received by node X is replayed through node Y and vice versa.

Normally it take several hops for a packet to traverse from a location near X to a location near Y, packets transmitted near X travelling through the wormhole will arrive at Y before packets travelling through multiple hops in the network. The attacker can make A and B believe that they are neighbours by forwarding routing messages, and then selectively drop data messages to disrupt communication between A and B [12].

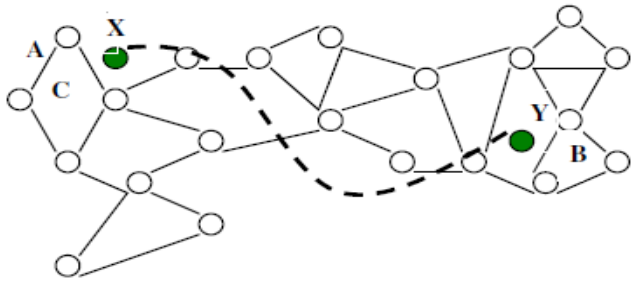

Figure 1: Wormhole Attack [13]

5. WORMHOLE ATTACK MODEL

Wormhole attack is one of the Denial-of-Service attacks that can affect the network even without the knowledge of cryptographic techniques implemented. This is the reason why it is very difficult to detect. It may be launched by one, two or more number of nodes. In two ended wormhole, packets are tunnelled through wormhole link from source to destination node. On receiving packets, destination node replays them to the other end.

Designing prevention and detection methods of Wormhole attack requires the classification of Wormhole attacks. Figure 2 illustrates the three models of wormhole attack.

Depending on whether the attackers are visible on the route, packet forwarding behaviour of wormhole nodes as well as their tendency to hide or show the identities, wormholes is classified into three types: closed, half open, and open. In the following cases S and D are the source and destination nodes respectively. Nodes M1 and M2 are malicious nodes.

5.1 . Open Wormhole

Source(S) and destination (D) nodes and wormhole ends M1 and M2 are visible. Nodes A and B on the traversed path are kept hidden. In this mode, the attackers include themselves in the packet header following the route discovery procedure. Nodes in network are aware about the presence of malicious nodes on the path but they would imitate that the malicious nodes are direct neighbours.

5.2 . Half-Open Wormhole

Malicious node M1 near the source (S) is visible, while second end M2 is set hidden. This leads to path S-M1-D for the packets sent by S for D. The attackers do not modify the content of the packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet

5.3 . Close Wormhole

Identities of all the intermediate nodes (M1, A, B, M2) on path from S to D are kept hidden. In this scenario both source and destination feel themselves just one-hop away from each other. Thus fake neighbours are created.

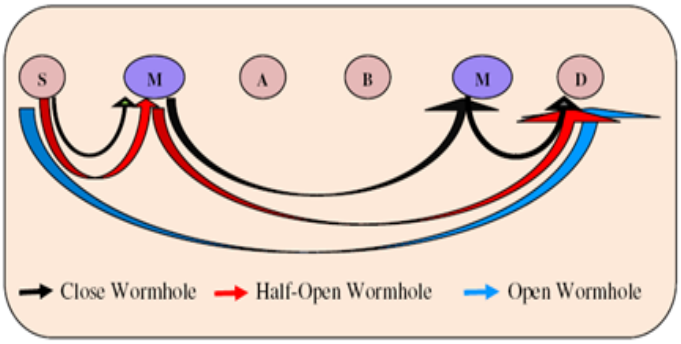

Fig 2: Representation of Open, Half-Open and Closed Wormhole [14]

6. TYPES OF WORMHOLE ATTACK

In this section, we classify the wormhole attack based on the techniques used for launching it. Number of nodes involved in establishing wormhole and the way to establish it classifies wormhole into the following types:

6.1 . Wormhole using Packet Encapsulation

Here several nodes exist between two malicious nodes and data packets are encapsulated between the malicious nodes. Hence it prevents nodes on way from incrementing hop counts. The packet is converted into original form by the second end point. This mode of wormhole attack is not difficult to launch since the two ends of wormhole do not need to have any cryptographic information, or special requirement such as high-power source or high bandwidth channel.

6.2 . Wormhole using Out-of-Band Channel

This kind of wormhole approach has only one malicious node with much high transmission capability in the network that attracts the packets to follow path passing from it. The chances of malicious nodes present in the routes established between sender and receiver increases in this case. Also this type is referred as “black hole attack” in the literature.

6.3 . Wormhole using Packet Relay

One or more malicious nodes can launch packet-relay-based wormhole attacks. In this type of attack malicious node replays data packets between two far nodes and this way fake neighbours are created. This kind of attack is also called as “replay-based attack” in the literature.

6.4 . Wormhole using Protocol Distortion

In this mode of wormhole attack, single malicious node tries to attract network traffic by distorting the routing protocol. This mode does not affect the network routing much and hence is harmless. Also it is known as “rushing attack” in the literature.

The following Table IV summarizes different modes of the wormhole attack along with the associated requirements are given [15].

Table 3. Summary of wormhole attack modes

Name of Mode	Minimum no. of adversary nodes	Requirements
Packet Encapsulation	Two	None
Out -of -band Channel	Two	High speed wire line link
High power Transmission Capability	One	High power source
Packet relay	One	None
Protocol Distortions	One	None

7. COUNTERMEASURES TO WORMHOLE ATTACK

Several Researchers have worked on detection and prevention of wormhole attacks in Wireless Sensor Networks. This section will describe the important wormhole attack detection mechanisms.

5.1.1 Location Information based method

Hu, Perrig and Johnson defined the wormhole attacks in adhoc networks [16]. Later, they proposed a mechanism, called packet leashes, which prevents packets from travelling farther than transmission range. This mechanism describes two types of leashes: Geographical and Temporal. In Geographical Leashes, each node knows its precise location and all nodes have loosely synchronized clocks to determine the neighbour relation. Before sending a packet, node appends its current position and transmission time to it. On receiving packet, receiving node computes the distance with respect to the sender and the time required by the packet to traverse the path. The receiver can use this distance information to deduce whether the received packet passed through a wormhole or not. In Temporal Leashes, every node maintains a tightly synchronized clock but does not depend on GPS information [11].

Both mechanisms use lightweight hash chains to authenticate the nodes [9]. The Message Authentication Code (MAC) can be calculated in real time. One benefit of packet leashes is the low computation overhead.

5.1.2 Statistical Analysis method

Song et al. propose a wormhole discovery mechanism based on statistical analysis of multipath routing. Song observes that a tunnel created by a wormhole is very attractive in terms of routing, and will be selected and requested with unnaturally high frequency as it only uses routing data already available to a node. These factors enables for easy integration of this method into intrusion detection systems only to routing protocols that are both on-demand and multipath [16].

5.1.3 Hardware based method

Hu and Evans suggested the method of directional antennas [17]. It is based on the fact that in ad hoc networks with no wormhole link, if one node sends packets in a given direction, then its neighbour will receive that packet from the opposite direction. Only when the directions are matching in pairs, the neighbouring relation is confirmed. It is necessary that each node requires a special hardware i.e. directional antenna.

5.1.4 Visualization based method

Multi-dimensional scaling-visualization of wormhole (MDS-VOW) is adopted by Wang and Bhargava [11] to detect wormhole attacks in static WSNs. In this approach using the received signal strength, every node measures the distance to its neighbour. Based on these measurements, base station calculates the network's physical topology. It is observed that the network with malicious nodes has different visualization from that with normal nodes. In absence of wormholes, topology should be more or less flat, where as in their presence 'string' pulling different ends of network are seen. It reconstructs the layout of the sensors using multi-dimensional scaling scheme. The anomalies, which are introduced by the fake connections through the wormhole, will bend the reconstructed surface to pull the sensors that are far away to each other. Therefore, MDS-VOW could locate the wormhole connections. In MDS-VOW, all sensor nodes are required to send their neighbour lists to the base station.

5.1.5 Graph theory method

Lazos and Poovendran [11] developed a "graph theoretical" approach to wormhole attack prevention in WSNs. According to it, limited location-aware guard nodes (LAGNs) which are nodes with known location and origination which can be acquired through GPS receivers are used. Between every one hop neighbours, LAGNs use "local broadcast keys". In order to detect wormhole attack, it is not possible to decrypt a message encrypted with a local key – encrypted with the pair-wise key. Hence during the key establishment, authors used hashed messages from LAGNs to detect wormholes. If a wormhole is present, node can detect certain inconsistencies in messages from different LAGNs. In absence of wormhole, a node should be unable to hear two LAGNs that are far away from each other.

5.1.1 Hop counting method

The hop count is the minimum number of node-to-node transmissions. This method uses protocol Delay per Hop Indicator (Delphi) [16] proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to determine every available disjoint route between a source and a destination. To identify wormhole, delay time and length of each route are measured and the average delay time per hop along each route is

computed. According to this, the route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both modes of wormhole attack; however, pinpoint the location of a wormhole cannot be determined.

5.1.2 Message Travelling time information based method

Message travelling time information is measured in terms of round trip time (RTT). One way to prevent wormhole attack, as used by Tran et al. [11], Jane Zhen and Sampalli [16], is to measure RTT of a message and its acknowledgement. The RTT is the time that extends from the Route Request (RREQ) message sending time of a node A to Route Reply (RREP) message receiving time from a node B. Node A will calculate the RTT between A and all its neighbours. Because the RTT between two fake neighbours is higher than between two real neighbours, node A can identify both the fake and real neighbours. In this mechanism, each node computes the RTT between itself and all its neighbours. No special hardware is required in this mechanism[16].

5.1.3 Trust based methods

Another significant method for identifying and isolating malicious nodes that create a wormhole in the network is Trust Based Method by Jain and Jain [16] .In this method, trust levels are derived in neighbouring nodes based upon their sincerity in execution of the routing protocol. This derived trust is then used to influence the routing decisions, which in turn guide a node to avoid communication through the wormholes. Assuming that wormholes drop all the packets it receives, it should have least trust level and hence can be easily eliminated. By using Trust Based Model Packet Dropping is reduced by 15% without using any cryptography mechanism and throughput is increased up to 7-8%.

Table 4. Summary of wormhole attacks detection mechanisms

Methods	Requirements	Comments
Temporal Packet Leashes by Hu, Perrig and Johnson[9]	Tightly synchronized clocks	Required time synchronization level and currently not achievable in sensor networks
Geographical Packet Leashes[9]	GPS coordinates of every node; Loosely synchronized clocks (ms).	Robust, straightforward solution; inherits general limitations of GPS technology
Statistical Analysis by Song et al[17]	Requires statistical routing information from each sensor node.	Works only with multi-path on-demand protocols; Easy integration with intrusion detection system
Directional Antennas by Hu and vans[10]	Nodes use specific 'sectors' of their antennas to communicate with each other; Directional antennas on all nodes.	Good solutions for networks depending on directional antennas, but not directly applicable to other networks.
Network Visualization(MDS-VOW) by Wang and Bhargava[11]	Requires central coordination	Works best on dense networks; Mobility is not studied
Graph theoretic model by Lazos and Poovendran[16]	Requires a combination of location information and cryptography	Uses location aware guard nodes equipped with GPS receivers
Travelling time mechanism by Tran et al.[18]	Does not require any special supporting hardware	Measures Round Trip Time of a message and its acknowledgement
Multipath Hop-count Analysis by Shang, Laih and Kuo[16]	No hardware requirement	Scheme has high efficiency and very good performance with low overhead
Trust Based Model by Jain and Jain[16]	No hardware requirements	Effectively locate dependable routes through the network

8. OPEN RESEARCH CHALLENGES

In the previous sections, we have studied various strategies of network layer attacks, significance of wormhole attack and their countermeasures in Wireless sensor networks. This section will identify open research challenges in this area. In Table 3, summary of wormhole detection technique is presented. Most of the methods employ hardware which increases the manufacturing cost of a sensor node. Later researchers focused on software-based wormhole detection techniques. But still the detection of wormhole attacks in sensor networks is a challenging task for researchers.

Among software-based methods, Multipath Hop count analysis, travelling time mechanism, trust based models are widely used as they are promising in terms of detecting wormhole attacks without any hardware requirements. As per these techniques, it is assumed that time or distance data used for wormhole detection cannot be changed. Since malicious nodes are able to modify transmitted information, distance-bounding and time-based wormhole detection techniques must be supported with cryptographic authentication mechanisms so that authenticity of the information can be verified over the path.

Wormhole attacks are strictly related to network layer protocols. As new routing protocols are proposed for WSNs, it is important to identify possible shortcomings of these new routing protocols, measure the performance of new routing protocol with wormhole attack and to investigate the effectiveness of the existing wormhole detection techniques on these protocols. Hence, there is a scope for further research in terms of measuring performance of existing wormhole detection techniques on new routing protocols. Future work in this area focuses on additional security enhancements for routing protocols in wireless sensor networks.

In the current wormhole detection research usually static topology of WSNs are considered. Hence, wormhole detection in a dynamic WSN is an open research area. In a dynamic WSN, any two genuine sensor nodes that were previously many hops far from each other may become one hop neighbours, and hence creates illusion for the base station that a wormhole attack has been launched. Hence, it is a challenging task to distinguish such genuine nodes from malicious nodes while detecting wormhole attacks.

9. CONCLUSION

Wireless sensor networks are vulnerable to wide range of security attacks because of their deployment in an open and unprotected environment. This survey paper introduces the major security threats in WSN and also investigates different wormhole detection techniques, examines various existing methods to find out how they have been implemented to detect wormhole attack. It has been studied that among the number of techniques discussed, each technique has its own strength and weaknesses and there is no proper wormhole detection technique that can detect all wormhole attacks completely. Finally, by analyzing the pros and cons of existing techniques, the open research challenges in the wormhole detection area are studied.

ACKNOWLEDGEMENTS

My sincere thanks to my honorable guide Prof. Niketa A.Chavhan and others who have contributed towards the preparation of the paper.

REFERENCES

[1] Kia Xiang, Shyaam Sundhar Rajamadam,Srinivasan, Manny Rivera,Jiang Li, Xiuzhen Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey", pp 1-28, Springer, 2005.

[2] G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security Vol. 4, No. 1 & 2, 2009.

[3] Nityananda Sarma , Sangram Panigrahi, Prabhudutta Mohanty and Siddhartha Sankar Satapathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, 2005.

[4] Abhishek Jain,Kamal Kant, "Security Solutions for Wireless Sensor Networks", IEEE Second International Conference on Advanced Computing & Communication Technologies, pp 430-433,2012.

[5] Shahriar Mohammadi and Hossein Jadidoleslamy, "A Comparison Of Link Layer Attacks On Wireless Sensor Networks", International journal on applications of graph theory in wireless ad hoc networks and sensor networks(GRAPH-HOC) Vol.3, No.1, March 2011.

[6] Sushma, Deepak Nandal, Vikas Nandal, "Security Threats in Wireless Sensor Networks", IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011.

[7] Syed Ashiqur Rahman ,Md. Safiqul Islam, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches", International Journal of Advanced Science and Technology Vol. 36, November, 2011.

[8] Ali Modirkhazeni, Norafida Ithnin, Mohammadjavad Abbasi, "Secure Hierarchal Routing Protocols in Wireless Sensor Networks: Security Survey Analysis", IJCCN International Journal of Computer Communications and Networks, Volume 2, Issue 1, February 2012.

[9] Dhara Buch, Devesh Jinwala, "Detection of Wormhole Attacks in Wireless Sensor Networks", IEEE Conference on Advances in Recent Technologies in Communication and Computing, pp 7-14, 2011.

[10] Khin Sandar Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.

[11] Majid Meghdadi, Suat Ozdemir and Inan Guler , "A Survey of Wormhole based Attacks and their Countermeasures in Wireless Sensor Networks", IETE TECHNICAL REVIEW, VOL 28, ISSUE 2, Mar-Apr 2011.

[12] Mani Arora, Rama Krishna Challa," Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, pp 102-104, 2010.

[13] Rama Krishna Challa ,Mani Arora, Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", IEEE Second International Conference on Computer and Network Technology, pp 102-104, 2010.

[14] Dhara Buch, Devesh Jinwala, "Prevention of wormhole attack in Wireless sensor network",International Journal of Network Security & Its Applications (IJNSA), pp 85-98, Vol.3, No.5, Sep 2011.

[15] Marianne Azer, Sherif El-Kassas, Magdy El-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks", International Journal of Computer Science and Information Security(IJCSIS), pp 41-52, Vol. No. 1, May 2009.

[16] Preeti Nagrath,Bhawna Gupta,"Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A survey", pp 245-250, IEEE 2011.

[17] Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao, Fuxiang Gao, "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis", IEEE International Conference on Information Engineering, pp 251-254, 2010.

[18] Prasannajit B, Venkatesh, Anupama S, Vindhykumari, "An Approach towards Detection of Wormhole Attack in Sensor Networks", IEEE First International Conference on Integrated Intelligent Computing, pp 283-289, 2010.

Authors

Priya Maidamwar received the B.E. degree from K.D.K College of Engineering, Nagpur, State-Maharashtra, India. She is pursuing Master of Engineering (M.E.) in Wireless Communication and Computing from G. H. Raisoni College of Engineering, Nagpur. Maharashtra, India. Her research area includes Wireless network security, Wireless sensor network.

Nekita Chavhan received the Master of Engineering (M.E.) in Wireless Communication and Computing from G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India. She is working as Assistant Professor in G. H. Raisoni College of Engineering, Nagpur. Her research area includes Ad-hoc Wireless networks, Wireless sensor networks and Mobile Technology.