Frequency Based Detection Algorithm of Wormhole Attack in WSNs

***Manisha, Computer** Science and Engineering Department, Shoolini University, Solan (HP),India.*
***Gaurav Gupta,** Computer Science and Engineering Department, Shoolini University, Solan (HP),India.*

Abstract
The main Importance of Research paper is to propose a new algorithm for the detection of wormhole Attack in the WSNs. Wormhole Attack is the severe attack on WSN routing protocols. Two malicious nodes create an illusion that they are very close to each other by setting up low latency link(wormhole tunnel), retrieve data packets on one part and transmit it to another part of the network via that wormhole tunnel. This allows an intruder to subvert the correct operation of routing protocols, by controlling the numerous routes in the network. Hence, this paper explains the Algorithm for Wormhole Detection in Wireless Sensor Networks, which detects wormhole tunnel based on the static Frequency (Bandwidth) parameter in a network. The important advantage of the Wormhole Detection algorithm is that it can detect the approximate presence of wormhole tunnels, which is useful in implementing countermeasures.

Index Terms: **Wireless sensor Networks, Wormhole Attack, MDS-VOW, FRDet Packet, Wormhole Tunnel**

I. INTRODUCTION

Wireless Sensor Networks are viewed as a network consisting of thousands of sensor notes (also called Motes) that are considerably monitored in hostile and Industrial environment[1,2]. These sensor Nodes perform several tasks as signal processing, sensing, and computational and network self-configuration to extend the network coverage and its scalability. Routing is the main processing to determine the secure path in the network and transmit the data confidentially and securely. Sensor Nodes work collaborates to collect the data and transmit that data from different nodes to base station and base station further transmit data to needy users. Because Wireless Sensor Networks are usually deployed in security environment and implement critical tasks, loss of availability may have serious impacts such as attacks, congestion, synchronization, packet loss and drop unconditionally.

Due to limited resources of Motes, open nature fast deployment and distributed network architecture of WSNs, make them vulnerable to wide range of security attacks at Network Layer. Wormhole attack is one of most complicated attack and several combinations of attacks (Sinkhole attack, black hole attack, Hello Flood attack and Selective Forwarding Attack), this attack is hard to detect and prevent.

In this attack, the malicious node capture the packets over a low latency link(wormhole link) and tunnel them to another malicious node far away, it makes two nodes far away believe that they are neighbors in one hop. The wormhole attack make adverse effect on secure location, data aggregation, network routing protocols. This attack is particularly challenging to deal with since the adversary does not need to compromise any legitimate nodes or have access to any cryptographic keys.

The rest of the paper is follows as:

Section II demonstrates the Significance of Wormhole Attack. Section III studies the solutions of Wormhole attack that had already implemented in past. Section IV presents our proposed algorithm to detect the wormhole attack and its results. Section V concludes the overall paper. Section VI presents the future scope of our proposed algorithm.

II. SIGNIFICANCE OF WORMHOLE ATTACK

Wireless Sensor Networks make vulnerable to several kinds of security attacks due to scarcity of various resources. Wormhole Attack is a kind 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.

Wormhole attack can be classified in two ways:

1. Exposed Wormhole: In this attack, Wormhole nodes impersonate as legitimate nodes which communicate with each other directly. Due to the exposed wormhole attack, nodes select the route which is created by malicious nodes rather than original route. And other nodes may get the same result. The attack makes this mistake.
2. Hidden wormhole: In this attack, nodes do not expose themselves in the wireless sensor networks. Hidden wormhole attacks need not compromise any node, and other nodes cannot feel the threat. By forward packets from one node to another. They do not need secret key of the networks. So, If the wormhole is placed carefully by an attacker and the transform distance is long enough, it can create many false routes (not only for the wormhole nodes but also beyond nodes) and have serious effects on routing protocols since it influences the topology construction. Based on the above analysis, the hidden wormhole is more serious which do not need any initialize conditions and information of the networks.

It should be noted that wormholes are dangerous by themselves, even if attackers are diligently forwarding all packets without any disruptions, on some level, providing a communication service to the network. With wormhole in place, affected network nodes do not have a true picture of the network, which may disrupt the localization-based schemes, lead to the wrong decisions, etc. Wormhole can also be used to simply aggregate a large number of network packets for the purpose of traffic analysis or encryption compromise. Finally, a wormhole link is simply unreliable, as there is no

ISSN: 2278 – 1323

way to protect what the attackers can do and when. Simply put the wormholes are compromising network security whether they are actively disrupting routing or not.

III. SOLUTIONS TO WORMHOLE ATTACK

A significant research has been done to detect wormhole attacks in WSNs. Many algorithms and mechanisms have been implemented to detect the wormhole attack in routing protocols such that packet leashes which are presented in [4, 5, 6, 7]. This technique categorized in two ways: geographic leash and temporal leash. This technique used physical metric, such as time delay or geographic location to detect the wormhole attack. Wang [12, 7] implement an approach inspired by packet leashes, but their system is based on end-to-end location information, rather hop-by-hop leashes. Hu and Evans present a technique to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas. SeRWA (Secure Route protocol against Wormhole Attack in sensor networks) has also been presented [13, 2]. This protocol didn't require any special hardware to detect wormhole attacks. Wang et al. [14, 7] propose a method named MDS-VOW [14, 7] that used multidimensional scaling to rebuild the network and detects the wormhole attack based on the distance of neighbors to a central server.

L. Lazes et al. [15, 7] propose another mechanism named LAGNs (Location –Aware 'Guard' Nodes) to prevent the wormhole attacks on wireless ad hoc networks based on the guard nodes. They acquire guard node to detect the message flow between nodes. A guard node can detect a wormhole attack using guard property and communication range constraint property during fractional key distribution. Design Dong [8] presented a distributed detection method which detects the wormhole attack based on topology. This method relies solely on network connectivity information.

S.Sharmila and G.Umamaheswari proposed the wormhole attack detection mechanism "Transmission Time based detection" [9] which used transmission time and hop to detect the wormhole attack. TIAN Bin, LI Qi, YANG Yi-Xian, LI Dong, XIN Yang propose ranging based detection mechanism to detect the wormhole attack in WSN. The topology of the network is static and nodes are randomly deployed. This scheme analyzed the time overhead from the node broadcast a message to the node receive from its neighbor echo the message and fake neighbor nodes. This technique used k-means cluster analysis to detect the wormhole attack detection that relies on the distance correlation in the physical location of nodes. The nodes are characterized in two clusters, say, legal nodes and illegal nodes [10]. Xiaopei Lu, Dezun Dong, and Xiangke Liao propose MDS (multidimensional scaling- based detection mechanism which detects the wormhole attack by only topology information. In this approach, the algorithm is described to detect the wormhole attack based on several parameters that influence the performance of this algorithm [11].

IV. PROPOSED MECHANISMS AND RESULTS

The existing algorithms are more resource hungry. In Transmission Time Based Mechanism, Many Problems arises such as Energy Consumption, Memory Overhead and Bandwidth Consumption which leads the performance degradation in WSNs.

This section represents the proposed mechanism to detect the Wormhole Attack in WSNs at Network Layer. In Previous Literature Review, many research papers have been published on the Wormhole Attack Detection mechanism in WSNs. By analyzing previous literature, we figured out that there is no any mechanism to detect the wormhole attack in WSNs using frequency parameter. Hence, we proposed a new mechanism to detect the wormhole attack in WSNs using Frequency parameter. The main concept in detecting presence of wormhole tunnel in a network is to find out if node is transmitted in safe route path or not. This Mechanism proposed that every node will maintain a frequency table by updating its all information after every process.

Two Main Characteristics of the Proposed work:

Frequency Table: Every node in the network will maintain a Frequency table which will consists of node ID, Route Path and Frequency of Route Path. As the network we are implementing is a uniform one hence the node will be in set in matrix format hence we can easily get the Frequency table.

Detection procedure: The algorithm detects wormhole tunnel in the network when it receives a FRDet Pkt. FRDet Packet is a packet that consist commands to detect the frequency of Active Route path which check that wormhole tunnel is exist or not based on condition that explained later. In this section, we conceive an algorithm based on frequency to detect the wormhole Attack in WSNs at Network layer.

Assumptions

In this Detection Algorithm we have assumed static Frequency the static frequency to transmit the data Packets on Route Path in WSNs. The network is based on hybrid topology that describes the structure and topological view of dynamic nodes.

Frequency Based Wormhole Detection Algorithm
Consider the Input Nodes{1…n}
Messages{M1…Mi}
Frequency Table→ Nodes, Frequency , Route Path
Initialize Frequency ,F→{fs,N}
Sender initiate RReqPkt + FRDetPkt{fv, N}
FRDetPkt-> "sudo iwlist wlan0 scan | grep Frequency |"
Passing Signal, P->{RReq, FRDet, F}
If (FRDet{fv,N}→ F{fs,N})
{
Return (1) or true
Transmission Allow
Send RRep +AckPkt to sender
}
Else
{
Return (0) or false
Transmission Block
(wormhole tunnel Exist)
Broadcast message to neighbor nodes + sender Node
}
Update Frequency Table

Develop a network that consist several nodes in a uniform way. Create Frequency Table consists Nodes, Route and Frequency of path.

ISSN: 2278 – 1323

Consider F as Frequency Function such as :

$F \rightarrow \{fs, N\}$

Where fs represents Static Frequency of Route Path
N represents the Node Path
Sender initiates RReqPkt to merge with FRDetpkt and broadcast this message to all nodes that are participated in the Network.
Consider FRDet as Frequency Detector Packet to detect the Frequency of Route Path such as

$$FRDet\ Pkt \rightarrow \{fv, N\}$$

Where fv represents Variable Frequency that are detect
To detect the wormhole Attack that is created by malicious node in the network. An FRDet Packet transmits in the network which scans all active route path and figure out all the frequencies that are currently occurred in the network. To detect the Frequency (Bandwidth) of Route Path, following commands are following as:
Sudo iwlist wlan0 scan | grep Frequency |
This command evaluates all frequencies of Route Path that exist in the network. After considering all Functions, the next step is to broadcast sender's message (RReqpkt + FRDet Pkt) to all nodes that are participated in the network. The Next step is to evaluate the condition for the indication of wormhole Attack in the network whether attack is in or not. The condition is applied as: FRDet (FRDet {fv, N}→ F {fs, N}, this Condition checks that the Frequency of the Active Route Path is same as static Frequency that we provide in the network. If this Condition is True, This simplify that Wormhole Tunnel Not Exist and Transmission allow in Safe Mode and Broadcast all data Packets on that Route Path by Sender and Other Participated odes with RRep Packet and AckPKt, otherwise, Transmission Block and Wormhole tunnel Exist in that Path.
After this, broadcast this Information to all other Nodes in the network and Frequency Table Updated with Fresh Data automatically and this whole process repeats in the active network.
Implementation Result:
The frequency detection Algorithm is implemented in C. the implementation of algorithm will be in wormhole section of the network hence the algorithm if run in the network will detect wormhole tunnel because the detection is using frequency packet information to detect wormhole in the network.
Set Frequency which is static and assume(E.g. 2.5 GHz) in the network.
Detect Frequency which comes by transferring the FRDet packet in the network.
Here is the output file of the above code section which represents the implementation part to detect the wormhole attack using Frequency parameter.
The output file consists two cases:
When both frequencies are same(Set and Detect Frequency). In this case, both frequencies are same which means that wormhole tunnel is not exists in the network as shown in Fig.1.

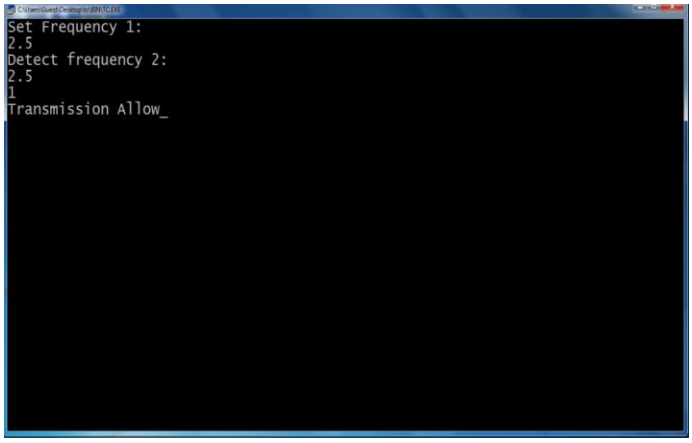

Fig.1 Implementation of Frequency based Algorithm
When both frequencies are different.
In this case, Set Frequency and Detect Frequency are alike, means that wormhole tunnel exists in the network as shown in Fig.2.

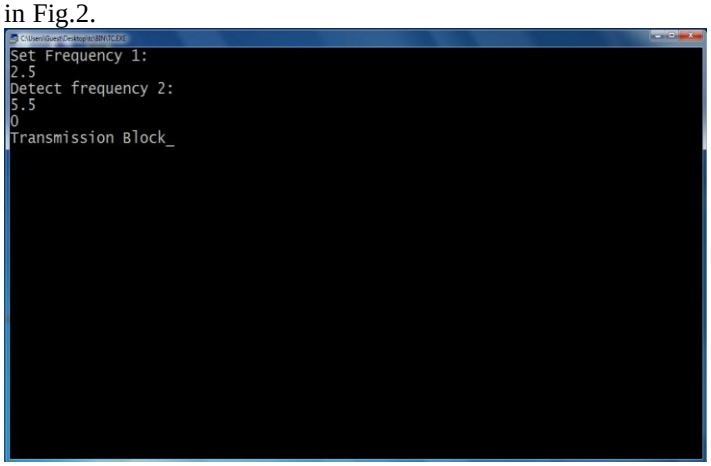

Fig.2 Implementation of Frequency based Algorithm

V. CONCLUSIONS

In WSN, each node in the network acts as a router (because they use broadcast mechanism), so as to create a secure routing protocol. Encryption and decryption techniques are used for secure routing. The algorithm is found to be less resource hungry as the algorithm only uses a simple search method to find the wormhole tunnel using Frequency (Bandwidth) Parameter in the WSNs and updating Frequency Table.

VI. FUTURE SCOPE

The Future Perspectives are following as:
The implementation of this algorithm with full hardware and software specification will give a very much real world scenario.
We will also intend to carry out the simulation in a Wireless Sensor Networks with the number of nodes and with the change in network dimensions.
To evaluate this algorithm with many routing protocols of WSNs and evaluate all the effects that will be carried out in the simulation setup.

REFERENCES

[1] Alzaid, Hani and Abanmi, Suhail and Kanhere, Salil and Chou, Chun Tung (2006), "Detecting Wormhole Attacks in Wireless Sensor Networks",

ISSN: 2278 – 1323

Technical Report, Computer Science and Engineering School - UNSW, the Network Research Laboratory - UNSW.
[2] Bin TIAN, LI Qi, YANG Yi-xian, LI Dong, and XIN Yang (June 2012), "A ranging based scheme for detecting the wormhole attack in wireless sensor networks", 19(Suppl. 1): 6–10, Springer.
[3] Dong Dezun, Mo Li, Yunhao Liu, Xiang-Yang Li and Xiangke Liao(2011), "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks", IEEE/ACM Trans. Networking, vol. 19, pp. 1787-1796.
[4] Garcıa-Otero Mariano, Adrian Poblacion-Hernandez (2012), "Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques", International Journal of Distributed Sensor Networks Volume 2012, Article ID 763187, 12 pages.
[8] Hu Y., A. Perrig, and D. Johnson (2004), "Packet Leashes: a Defense against Wormhole Attacks in Wireless AdHoc Networks", In proceedings of INFOCOM.
[10] Kenyeres J., M. Kenyeres, M. Rupp, P. Farkas (Sept 2013), "Connectivity-Based Self-Localization in Wsns", Radioengineering, Vol. 22, No. 3.
[11] Lazos L., R. Poovendran, C. Meadows, P. Syverson, L.W. Chang(March 2005), "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", In Proceedings of Wireless Communictions and Networking Conference, IEEE, pp.1193-1199.
[12] Lu Xiaopei, Dezun Dong, and Xiangke Liao(2012), "MDS-Based Wormhole Detection Using Local Topology in Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume, Article ID 145702, 9 pages doi:10.1155/2012/145702.
[13] Maidamwar Priya, Nekita Chavhan (October 2012), "A Survey On Security Issues to Detect Wormhole Attack in Wireless Sensor Network", International Journal on AdHoc Networking Systems (IJANS), Systems (IJANS) Vol. 2, No. 4, October 2012 DOI : 10.5121/ijans.2012.2404 37.
[14] Manisha, Gaurav Gupta, (October 2013) "Attacks on Wireless Sensor Networks: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 3, Issue 10, ISSN: 2277 128X.
[15] Meghdadi Majid, Suat Ozdemir and Inan Giiler (2011),"A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Network", IETE Technical review, Vol.28, Issue.2, PP89-102.
[16] Padmavathi, G., &Shanmugapriya, D. (2009), "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security (IJCSIS): Vol.4, No.1 & 2.
[17] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori and Ramjee Prasad(2012),"Behavioural Modelling of WSNs MAC Layer Security Attacks: A Sequential UML Approach", journal of Cyber Security and Mobility, 65–82,River Publishers
[18] Sharif Lukman and Munir Ahmed (June 2010), "The Wormhole Routing Attack in Wireless Sensor Networks", Journal of Information Processing Systems, Vol.6, No.2, and DOI: 10.3745/JIPS.2010.6.2.177.
[19] Sharmila S., G.Umamaheswari (August 2012), "Transmission Time based Detection of Wormhole Attack in Wireless Sensor Networks", Special Issue of International Journal of Computer Applications (0975 – 8887) on Information Processing and Remote Computing – IPRC.
[20] Tun Zaw and AungHtein Maw (2008), "Wormhole Attack Detection in Wireless Sensor *Networks"*, World Academy of Science, Engineering and Technology Vol: 22 2008-10-22.
[21] Wang W., B. Bhargava, Y. Lu and X. Wu(June 2006), "*Defending Against Wormhole Attacks in Mobile Ad Hoc Networks"*, Wireless Communication and Mobile Computing, Volume 6, Issue:4, pp.483-503.
[22] Wang W. and B. Bhargava (2004), "*Visualization of Wormholes in Sensor Networks*", In Proceedings of the ACM workshop on Wireless security (Wise'04), pp. 51-60.
[23] Weichao W., B. Bharat, Y. Lu, X. Wu, Wiley Interscience (2006), *"Defending against Wormhole Attacks in Mobile Ad Hoc Networks"*, Wireless Communication and Mobile Computing.
[24] Wood, A. &Stankovic, J. (2002), *"Denial of service in sensor networks",* In Computer. Vol 35, pp 54 –62.

ISSN: 2278 – 1323