Prevention of Wormhole Attacks in Wireless Sensor Networks

[1]Dema Aldhobaiban , [2]Khaled Elleithy and [3]Laiali Almazaydeh

[1,2] *Department of Computer Science and Engineering,* University of Bridgeport, Bridgeport, CT 06604, USA
[3] *Department of Software Engineering,* Al-Hussein Bin Talal University, Ma'an, Jordan
Daldhoba@my.bridgeport.edu , elleithy@bridgeport.edu, lalmazay@my.bridgeport.edu

***Abstract*- Security of deployed wireless sensor networks (WSNs) has become a crucial task as the deployment of WSN'S grows. This paper proposes a novel way and develops a mechanism to prevent wormhole attacks by an algorithm to manage a large number of nodes using node ID. Also, the proposal creates a load balancing feature for monitoring a hierarchical system for nodes and extra packet header on each node to make sure it is not compromised. Even though an attack is inevitable on a live node network using a simulator, this paper has shown how the network nodes can be rerouted to avoid the attacked nodes.**

Keywords: wireless sensor network, security, routing attack, wormhole attack, node ID.

I. INTRODUCTION

A sensor node is also called as mote. In a wireless sensor network, a node is capable to perform the processing, and gathering of the sensor information for communication with all other connected nodes in the network. Sensors are the hardware devices: they measure and produce a proper response by a physical condition like pressure or temperature. Sensors are monitored by using a physical data parameter. Generally, a sensor is small in size to consume low energy and volumetric densities that operates adaptive environment.

Node is applicable in the mobile applications that are transmitted by Application Programming Interface. In wireless networks, sensors challenge several characteristics, constraints, and distinguish the contemporary communication. Sensor nodes are tightly constrained in the terms of energy, power, and bandwidth storage capacity.

Security is the major problem in wireless sensor networks. Wormhole attacks can make the network vulnerable. A wormhole attack means a node illegitimately claims multiple nodes. This attack threatens wireless sensor networks in routing, voting system, fair resource allocation, data aggregation, and misbehavior detection .The research is carried out to prevent the wormhole attacks and improve the network performance The node ID-based scheme is proposed, where the detection is based on node registration, consisting of two phases and the assignment of ID to the node is done dynamically. The ID's corresponding to the nodes registered is at the base station, and the node active time is monitored. Any abnormalities in the above phases confirm the presence

of damaged and attacked nodes in the network. The algorithm will be simulated using C#. The energy consumed for this algorithm will also be calculated. The proposed detection algorithm is analyzed based on the network's Physicians' Desk Reference (PDR) and found that the throughput has improved, which prove that this algorithm may be used in the environment where security is needed.

II. RELATED WORK

Advancement in Wireless Sensor Networks (WSNs) and Micro-Electro Mechanical Systems (MEMS) have continued to impact daily life from performance of complex tasks such as monitoring life signs in hospitals to simple tasks such as monitoring temperature. In this new field of design, WSNs provide many applications such as military applications and creation of context aware homes. An example of such an application is Smart Dust. This new design on the other hand faces many challenges which for a long time were not considers feasible until the recently. Creating an organizational structure is one of the problems of the design. Researchers have come up with different ways of creating the organizational structures (clusters) because the WSNs have not been feasible in organizing the nodes. Clustering is a significant phenomenon in the organizational structure. Clustering forms an essential part in the WSNs in the organizational of the network that constituted of sensory nodes, clusters, cluster heads, base stations, and end users.

Clustering considers the limitation of WSNs such as limited energy, network lifetime, limited liabilities and application dependency in affecting the performance of the network. Implementation of WSNs poses great challenges because the traditional designs have little basis. Clustering algorithm is very essential in classified heuristic, weighted, hierarchical, and grid schemes. There are many heuristic algorithms that are used in choosing cluster heads such as linked cluster algorithm(LCA), linked cluster algorithm 2(LCA2),highest connectivity cluster, and max-min D cluster algorithm. In this d-hop max –Min provides the overall characteristic as compared to the other heuristic algorithms. This is because it produces a smaller number of cluster heads, larger clusters and longer duration of cluster heads as compared to LCA. In weighed Schemes, there are weighed clustering algorithms (WCA), clustered election procedure, and complexity due to distributiveness.

Hierarchical schemes include low-energy adaptive clustering hierarchy (LEACH), two level hierarchy LEACH (TL-LEACH), and energy efficient clustering scheme (EECS), and hybrid energy efficient distributed clustering (HEED).

For location and time based approaches, Hu, Perrig, and Johnson [1] demonstrated a method that relied on Packet Leashes, where geographic leash and temporal leash are placed on upper bound location of the receiver and maximum possible time frame needed for journey of packet, and the temporal lash is dependent on TIK protocol and ideas of geographical and time management are required.

Taheri, Naderi, and Barekatain [2] utilized leashes process with an enhanced packet distributor system to reduce measurement costs of TESLA with Instant Key Disclosure (TIK) protocol. In case of (TTM), Tran, Hung, and Lee brothers [3] came up with a method where every node is in place of path notes during transmitting RREQ packet while collecting RREP packet and time frame is also important. Singh and Vaisla [4] made an improvement by switching sender and receptor against manipulating response and proposal packet time rate. Hu and Evans [5] provided a method where the locating antenna can check details of neighbors by analyzing locations of HELLO messages and detecting neighbors by verifiers. Interestingly, this system can identify a threat from a spy by coming up with definite pair of confidential keys, but help from hardware is a must and wormholes with unreal neighbors can be identified with this process.

For locating wormhole threats, Khalil, Bagchi, and Shroff [6] had lightweight countermeasure (LITEWORP) with security nodes and subsequently wormhole, LITEWORP goes out of signal from that unlocked node only and increases chances of blockades to solve this a protocol called MOBIWORP [7], which had the ability to get rid of threatening nodes by central power from regional or international. Chen, Lou, and Wang [8] came up with a protected method for identifying simplex and duplex wormhole threats with a longer algorithm [8] for upgrading it to tackle non-identical distribution length of sensory nodes. Unfortunately, more than one wormhole can't be identified this way. Nait-Abdesselam, Bensaou, and Taleb [9] elaborated on identification and evasion system based on load support with diverse courses, and because of crowded packets, it has a hefty load and might give wrong alerts. Khurana and Gupta [10] , [11] suggested method was about total span and utmost scope of nodes SEEEP [10] but had drawbacks to nodes with similar distribution span which was elongated as FEEPVR [11] to help non-identical range or span.

Hayajneh, Krishnamurthy, and Tipper [12] proposed SECUre NeighborhooD (SECUND) protocol for detecting more than one wormhole without required ideas about node locality, and clock management and does not need unique hardware equipment but only performs when wormhole augment unreal neighbors by a bigger number. Dimitriou and Giannetsos [13] had an algorithm based on linkage data and identified wormholes and works on locality routes present assay when it finds up to date nodes. Gupta, Kar, and Dharmaraja [14] submitted a method which can identify wormholes by calculating jumps or hop distinctions among neighbors that are nodes of single jump or hop away and had unique hand packets which detain analysis. Vani and Rao [15] suggested Wormhole-Evasion Route Reply decision packet (WARRDP) which exposes wormholes and ejection by fused process of hop calculation anomaly based and neighbor list processes.

Wang and Bhargava [16] proposed Multi-Dimensional Scaling- Visualization of Wormhole (MDS-VOW) with central manipulator and is a centralized system without aid of hardware equipment but works less for sparse network or linkage. P. Radha, L. Loukas [17] proposed a graph method which gives out probable features for locating and protection from wormhole threat with a unique guard node a longer radio span. Choi, Kim, Lee, and Jung [18] have come up with a Wormhole Attack Prevention (WAP) algorithm Dynamic Source Routing (DSR) protocol which functions perfectly for secret threats, but for present threats, it is not competent. Azer, Kassas and Soudani [19] had advanced a well-functioning locator and evade method on Diffusion of Innovations, but carriage time of both ends is augmented. Finally, Poornima, Bindu and Munwar [20] implemented a technique on geographic location with reverse.

III. PROPOSED APPROACH

An approach for the wormhole prevention is presented in this section with each node having a unique id linked to the surrounding nodes in a binary tree structure. To get the best optimal results of the experiment, derive a clustering based approach were in the affected node id, and its neighboring nodes links are severed from the rest of the node structure. Figure 1 shows the links with the red nodes effected and the purple links show the neighboring nodes. The green circular node is the source node that was infiltrated for the attack. In this approach we severed the nodes connected to the source node as well as the consecutive neighboring nodes. In the following case node {1, 3, 7, and 9} are also severed from the rest of the network to keep the infected nodes at bay.

Routing Scheme (RRS) also Authentication of Nodes Scheme (ANS), for identifying wormholes operates for BSR protocol, but the witness capacity is too serious. Attir, Abdesselam, Brahim, Bensaou, and Ben-Othman [21] presented a method by neighborhood identification by W-Delay with extra data to HELLO packet for exposing wormhole but is restricted to OLSR protocol with its neighboring nodes.

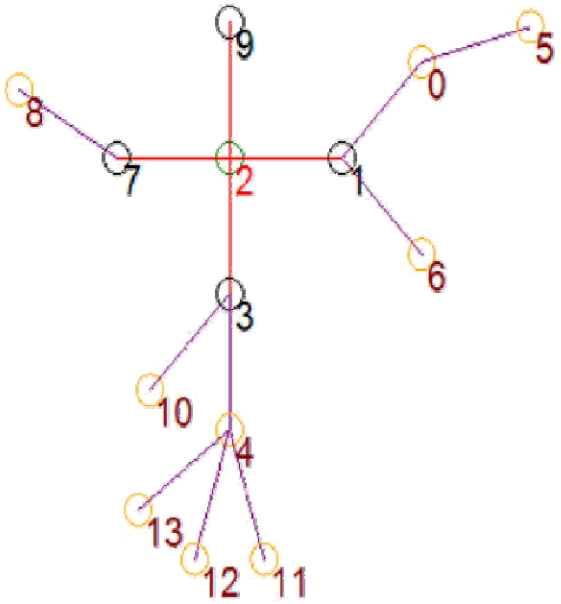

Figure 1: Neighboring Node Structure under Attack

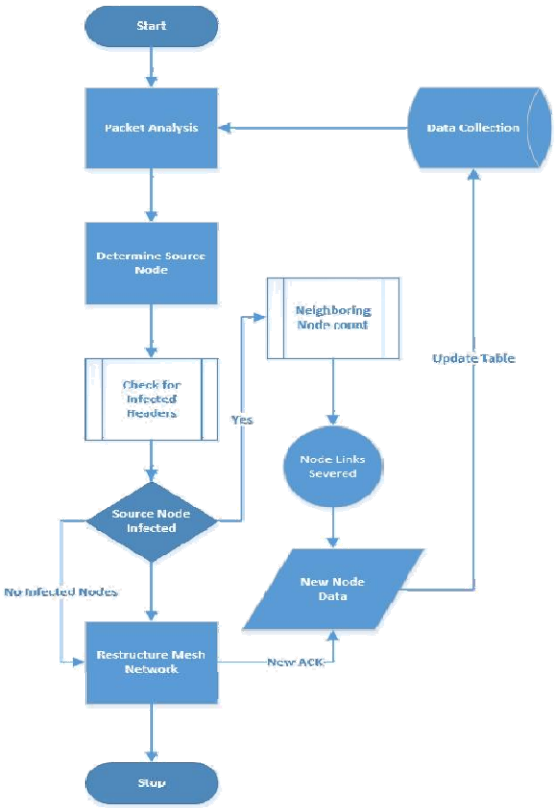

Figure 2: Flowchart depicting the proposed algorithm

Figure 2 shows the algorithmic approach, where each acknowledgement has a packet analysis done for the incoming data packets. The analyzed packets determine if any affected nodes in the mesh network. Since each node has a node id, it is easy to locate the infected node. A neighboring count is done on the infected node and all the links to and from the neighboring nodes are severed from rest of the mesh network. The mesh network data table is updated and the same process is run again until the whole mesh network is clear of all the infected nodes.

IV. SIMULATION AND RESULTS

The experiment developed a simulation using c# programming in windows form to simulate only the binary structure of how the nodes are severed in a mesh network and the source node connected along with the node ids. The process inputs a basic building block to display the node structure. Figure 3 depicts the simulation. The process can input the number of nodes and the neighboring nodes for each node in the network and simulate the results. The output displayed is just for ten nodes with six neighboring nodes. Since the increase in the number nodes makes the view unclear, this is just for the display purpose. The algorithm can run simulations of up to 100 nodes at a time with 8 neighboring nodes that in a total of up to 1000 nodes.

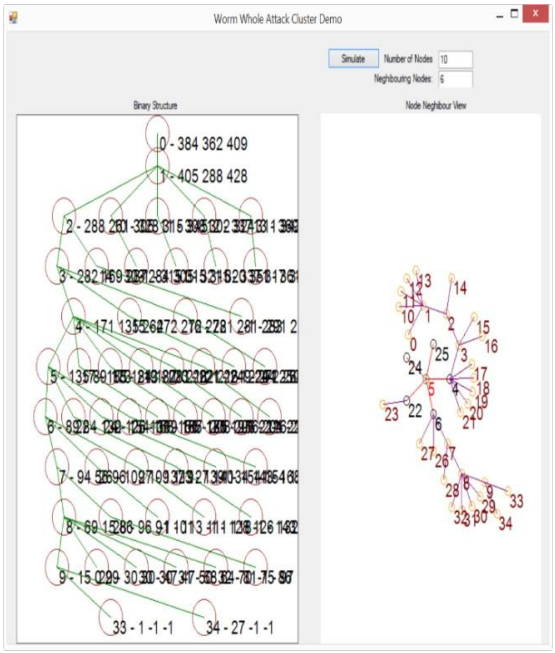

Figure 3: Simulation for Wormhole attack

The left window depicts the binary structure as to how the nodes are linked to each other using their node ids in the mesh network. The binary structure indicates which node subsets were infected in the mesh network. The right window depicts infected node in the mesh network. The

green node is the source infected node, and the red lines leading outwards from the source node show the links that are affecting the neighboring nodes. The purple links depict the secure and unaffected links. The black nodes are the ones that will also be severed from rest of the network as they are in immediate vicinity of the infected node. This way eliminate a small number of nodes in and around the infected node in a mesh network makes the whole mesh network secure.

Figure 4 shows that the new network throughput increased every time an infected node is found. The infected node is severed from the network, and the data table of the mesh network is updated and same throughput of nodes are run up until the infected nodes are found. The following is the result behind the increase in the throughput during the time for simulating a packet that was already severed the infected node from the network. The power will turn off then and will turn on the new mesh network, and attack nodes were turned off for shorter during this time.

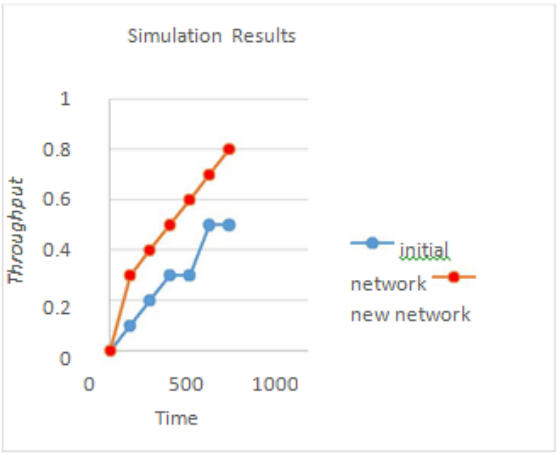

Figure 4: Graphical Result

V. CONCLUSIONS

This research paper has shown a novel way of securing a mesh network from wormhole attacks. The deletion of the links for the infected node and its neighbor leads to the security of the rest of the node network. Since this approach requires a table to monitor all the nodes, the load on the network is overwhelming. Thus to improve this, further experiments are planned to use more than one routing table in a very large mesh network. It will be similar to how routers help in routing algorithms by keeping information of its data sets in and around its vicinity.

REFERENCES

[1] Y. C. Hu, A. Perrig and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Wireless and Mobile Communications. ICWMC'08, pp.13-18, 2008.

[2] M. Taheri, M. Naderi and M. Barekatain , "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks," Proc. of IEEE International Conference on Communications, Vol. 10, pp. 3201–3205, June 2001.

[3] P.V. Tran , L. X. Hung ,Y.K. Lee, S. Y. Lee and H. Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks ," 4th IEEE conference on Consumer Communications and Networking Conference, pp. 593-598, 2007.

[4] A. Singh, K. S. Vaisla "A Mechanism for detecting Wormhole Attacks on Wireless Ad Hoc Network," International Journal of Computer and Network Security, Vol. 2, no. 9, pp. 27-31, September 2010.

[5] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," Network and Distributed System Security Symposium (NDSS), February2004.

[6] I. Khalil, S. Bagchi and N. Shroff, "LITEWORP: A Light weight Counter measure for the Wormhole Attack in Multi hop Wireless Network , "International Conference on Dependable Systems and Networks(DSN), pp.1-22, 2005.

[7] I .Khalil, S. Bagchi and N. Shroff , " MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks," nternational Conference on Depend able Systems and Networks(DSN), pp. 1-12, 2006.

[8] H. Chen, W. Lou, Z. Wang, "SLAW: Secure Localization against Wormhole Attacks Using Conflicting Sets," Technical Report, The Hong Kong Poly technic University, pp.111, 2010.

[9] F. Nait-Abdesselam, B. Bensaou and T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks, "Wireless Communications and Networking Conference, pp.3117-3122, 2007.

[10] N .Gupta and S. Khorana, "SEEEP: Simple and efficient end-to-end protocol to secure ad hoc networks against wormhole attacks," Fourth International Conference on

[11] N .Gupta and S.Khurana, "FEEPVR: First End-to- End protocol to Secure Ad hoc Networks with variable ranges against Wormhole Attacks," Second International Conference on Emerging Security Information ,Systems and Technologies –SECURWARE '08, pp.74-79, 2008.

[12] T. Hayajneh, P. Krishnamurthy and D. Tipper, "SECUND: A Protocol for SECUre NeighborhooD Creation in Wireless Ad hoc Networks," 5th International Conference on Collaborative Computing: Networking, Applications and Work sharing, Vol.1, no.2-3, pp.1-10, 2009.

[13] T. Dimitriou, A. Giannetsos, "Wormholes no more? Localized Wormhole Detection and Prevention," Wireless Networks in Distributed Computing in Sensor Systems -DCOSS, pp.334-347, 2010.

[14] S. Gupta, S. Kar and S. Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet," International Conference of Innovations in Information Technology, pp. 226-231, 2011.

[15]A. Vani, D. S. Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing in Ad Hoc Wireless Networks," International Journal on Computer Science and Engineering (IJCSE), Vol.3 No. 6, pp. 2377-2384, June 2011.

[16]W .Wang, B. Bhargava, "Visualization of wormholes in sensor networks," Proceedings of the 3rd ACM workshop on Wireless security, pp.51-60, 2004.

[17]P. Radha, L. Loukas , "A Graph Theoretic Frame work for Preventing the Wormhole Attack in Wireless Ad Hoc Networks" , Wireless

Networks Journal, vol .13, no.2-3, pp.27-59, 2007.

[18]S. Choi, D. Y. Kim, D. Lee and J. Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," IEEE International Conference on Sensor Networks, Ubiquitous, and Trust worthy Computing, pp.343-348, 2008.

[19]M. A. Azer, S. M. El-Kassas and M. S.El- Soudani, "An innovative approach for the wormhole attack detection and prevention in wireless ad hoc networks," International Conference on Networking, Sensing and Control (ICNSC), pp.366-371, 2010.

[20]E. Poornima, C. Shobha Bindu and SK. Munwar, "Detection and Prevention of Layer-3 Wormhole Attacks on Boundary State Routing in Ad Hoc Networks ," International Conference on Advances in Computer Engineering, pp.48-53, 2010.

[21]A. Attir, F. Nait-Abdesselam , B. Bensaou and J. Ben-Othman, "Logical Wormhole Prevention in Optimized Link State Routing Protocol," Global Telecommunications Conference, pp. 1011-1016, 2007.