Journal of Advanced Computer Science & Technology, 4 (1) (2015) 95-102
www.sciencepubco.com/index.php/JACST
©Science Publishing Corporation
doi: 10.14419/jacst.v4i1.4100
Research Paper

A cluster based approach for wormhole attack detection in wireless sensor networks

Maliheh Shahryari*, Hamid Reza Naji

College of Electrical and Computer Engineering, Graduate University of Advanced Technology, Kerman, Iran
**Corresponding author E-mail: maliheh.shahryari@gmail.com*

Abstract

Due to the need of cooperation among nodes to relay packets, wireless sensor networks are very vulnerable to attacks in all layers of the network. One of these severe attacks is the wormhole attack. Detection of wormhole attack is hard, because it can be easily implemented by attacker without having knowledge of nodes in the network or it can be compromised by any legal node in the network. To date, the most of proposed protocols to defend against wormhole attacks are made by adopting synchronized clocks, directional antennas or strong assumptions in order to detect wormhole attacks.
A method based on clustering is presented in this paper to detect this type of attacks. This method is implemented in static and mobile networks. The superiority of our protocol is that during the attack prevention or attack detection, the malicious nodes are detected and requires no additional hardware or complex calculations. Simulation results are perused with the NS-2 simulator and the protocol has been evaluated in terms of packet drop ratio, throughput, delay and energy consumption compared to a network without or under attack. Simulation results show that our protocol is practical and effective in improving resilience against wormhole attacks.

Keywords: *Wireless Sensor Network; Wormhole Attack; Clustering; Attack Detection.*

1. Introduction

Wireless Sensor Networks (WSN) consist of small, independent, autonomous and distributed devices that together monitor environmental or physical conditions in remote and often hostile environments. Wireless sensor networks have several unique features that distinguish them from traditional wireless networks. First of all, generally wireless sensor networks operate in unattended environments containing a large number of sensor nodes. These nodes are limited in terms of resource (energy, memory, and computation) [1], [2].
Another unique feature is the security of wireless sensor network. The important issue of security is although by developments of technology there is ability to design and implement new ways to increase security; network advances can use such developments to design new attacks. These attacks can include message modification, fabrication, black hole attacks, rushing attacks, etc. [3], [4].
One of the severe attacks is the wormhole attack, which has been introduced in the context of ad hoc networks. In this attack, a malicious node captures packets from one location in the network and ‘‘tunnels’’ them to another malicious node at a distant point, which replays them locally. This makes the tunneled packet arrive either sooner or with a lesser number of hops compared to the packets transmitted over normal multi-hop routes, as illustrated in Fig. 1.
In addition, it may affect data aggregation, clustering protocols and location-based wireless security systems. The wormhole attack can be launched even without having access to any cryptographic keys or compromising any legitimate node in the network [5].

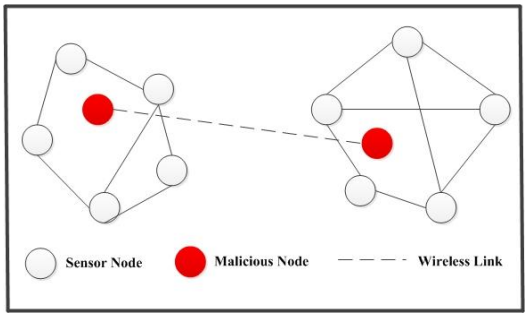

Fig. 1: Wormhole Attack.

Wormhole attacks can relay neighbor discovery packets to other areas of the network, trying to make distant nodes believe they are true neighbors. Once this is achieved, attackers are able to control other networking mechanisms like routing or topology-control algorithms, and manipulate nodes to send more traffic through them; this traffic may then be dropped or recorded enabling other kind of attacks such as the Sinkhole attack [6]. If the wormhole is placed carefully by the adversary and is long enough, it is easy to see that it can attract a lot of routing paths in the network.
It should be noted that wormholes are dangerous by themselves, even if attackers are continuously forwarding all packets, without disruptions at any level. With a wormhole in place, adversaries can just aggregate a large number of network packets for the purpose of traffic analysis or encryption compromise. Simply put, wormholes are unreliable and can compromise a network's security whether they are actively disrupting routing or not [7].
There are different ways to launch wormhole attacks in a wireless network environment which include using high power transmission, tunneling using encapsulation, tunneling using out-of-band channels, packet relay or protocol deviation [8].
The remainder of this paper is organized as follows. In Section 2, we present the related works done by the different authors. Section 3, presents our proposed protocol including system assumptions, notations, attack model and proposed algorithm. In Section 4, we present simulation-based results. Section 5, concludes the paper and presents further studies about the proposed protocol.

2. Related works

The most of proposed protocols to defend against wormhole attacks in wireless networks are made by adopting synchronized clocks, positioning devices, directional antennas or strong assumptions in order to detect wormhole attacks. This requirements and assumptions limit the applicability of network especially in the case of mobility.
Bin et al. (2012) introduced a statistical detection scheme. Their basic idea was that the presence of a wormhole strongly affects routing values and statistics information. This method relies on the time gained by the wormhole nodes that is higher than normal nodes. A threshold is considered that if the time is greater than the threshold, that node is considered suspicious node. In this protocol it is consumed that there is no wormhole along collecting statistics information and this information doesn't change due to node mobility [9].
Barman Roy et al. (2009), use a cluster-based approach for attack detection. In their approach, two layers were defined. Inner layer consists of non-cluster head nodes and a number of cluster heads. Also guard nodes are used to monitor the activities of all the nodes in the network. This algorithm is suitable for networks with heterogeneous nodes. If malicious node convinces cluster head in inner layer, detection is not possible [10].
Overall, in these approaches, nodes may frequently need to access a special node. This could cause a bottleneck and act as a single point of failure. Moreover, although they can inform us about the probability of a wormhole, they cannot extract the location of the link or which nodes are affected.
Qazi et al. (2013) presented a security enhancement to dynamic source routing (DSR) protocol against wormhole attacks for ad hoc networks which relies on calculation of round trip time (RTT). This method needs synchronized clock between nodes, it has large overhead and it is not effective for large-scale networks. Also, it is only used in static networks [5].
Shi et al. (2013), proposed a method to detect and isolate wormhole attacks in mobile ad hoc networks (MANETs). This method utilizes analytical hierarchy process to elect some special nodes, named the local most trustable (LMT) nodes, for the source and the destination node, respectively. Then the elected nodes are required to implement proposed scheme to prevent wormhole attacks. A LMT node is the node with the largest weight value in the vicinity of the source or the destination. The decision for the election of LMT node involves many metrics, including relative stability (S_r), credit value (C_v) and reciprocal of forward rate (R_f), which need to be traded off. The LMT nodes then perform the countermeasure to prevent wormhole attacks. This scheme has an overhead to calculate the weight value. Also, when a node moves to a new neighborhood, the node becomes a stranger to its neighbors. Hence, the node's weight value must be recalculated, and the problem mentioned above may arise again. If the node moves frequently, this problem may become more serious [6].

Stoleru et al. (2012), proposed a Secure Neighbor Discovery Protocol (MSND) that using mobile nodes determine whether two nodes are neighbors or not. The disadvantage of this method is that the mobile node moves in a specified direction and time of implementation of this protocol is also long [11].
In general, most of the above described protocols have some major shortcomings with respect to the processing and propagation delay times of transmitted packets and/or challenge requests–responses. In wireless networks, the MAC protocol always causes unpredictable delays. Thus, the detection metric is not expected to be very accurate which may lead to a large number of false positives. More importantly, these protocols cannot detect physical layer wormholes or wormholes that do not cause any delay.
Lazos et al. (2005) and Hu et al. (2004) proposed the use of directional antennas. The basic idea is to have neighboring nodes identified by zones which, in turn, are defined by directional antennas. The zones around each sensor are numbered 1 to N clockwise. When a sensor node receives a signal from another node, for the first time, it can get the approximate direction of the signal and identify the unknown originator by its zone. After that the sensor can cooperate with its neighboring nodes to verify the legitimacy of the unknown node [12, 13]. Such approaches are viable, but cannot be easily applied to sensor networks as they add expense, complexity, and special customized hardware. Also it is possible for an attacker to use adversarial nodes equipped with the same hardware in an attempt to deceive the detection protocol.
Giannetsos et al. (2013), presented a novel lightweight countermeasure for the wormhole attack, called LDAC (Localized-Decentralized Algorithm for countering wormholes). This method uses connection information (connectivity graph) and indicates that the attack has happened or not. The algorithm determines whether the distance (hop) of a node to its potential neighbors is smaller than the 2k hops or not, that k represents the information (hop) available from each node and usually is 1 or 2. This means that each node has its own 1 or 2 hops neighboring information. If this distance is greater than 2k hops, it means that there is other node (s) between the two nodes and the wormhole attack has happened [8].
While this is a nice, localized approach that does not require any time/location information or additional hardware, it suffers from a number of shortcomings. First, it depends on the network density and requires high connectivity. Second, detection is not always guaranteed without the availability of a specific number of independent nodes. Finally, the technique will probably fail when the average neighborhood size is low.

3. Proposed protocol

This model considers an adversary that can be (i) a legitimate node in the network, (ii) mount a “stealthy” wormhole attack. The wormhole is a dedicated connection, controlled by the attacker, between two physical locations in the network (wormhole endpoints). The main purpose of attacker is misleading the clustering protocol. Also, malicious node can disrupt the communication between cluster heads and be able to attract traffic. In more details, we show that our protocol prevent malicious nodes from performing these tasks and detect wormhole attack.
Proposed method describes an algorithm in which the intrusion detection is performed based on clustering method to detect wormhole attacks. The performed clustering is based on the l M-Leach protocol. Time is divided into parts of equal length called round. Each round consists of four phases: setup phases, member’s verification phase, cluster head routing phase and steady state phase. Fig. 2 shows the division of time in this protocol.

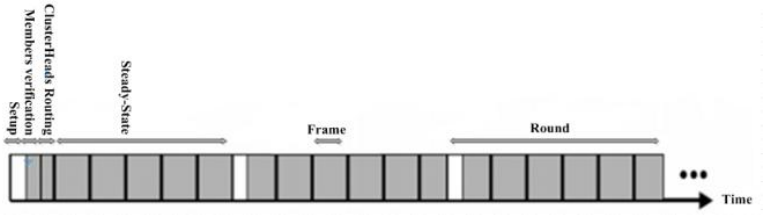

Fig. 2: The Division of Time in Proposed Protocol

The entire network is divided into clusters. Each cluster has its own cluster head (CH) and a number of nodes designated as member nodes (non-CH). Member nodes send the information only to the cluster head. The cluster head is responsible for passing on the aggregated information to all its members. The cluster head is elected dynamically and maintains the routing information.
In the setup phase, the nodes are organized in clusters. The cluster heads are determined with respect to the residual energy and mobility of nodes (nodes can be mobile). Each cluster head selects a number due to the residual energy and its mobility, if that number is smaller than the threshold value defined in equation 1, the sensor node is selected as cluster head in that round. The threshold is based on number of times a node has been cluster head, amounts of residual energy in the nodes and the node mobility.

$$P_i(t) = \begin{cases} \dfrac{p}{1 - p \times (r \bmod \frac{1}{p})} & \text{if } (C_i(t) = 1) \\ 0 & \text{if } (C_i(t) = 0) \end{cases} \quad (1)$$

In the above equation, p is recommended percentage for the number of cluster heads for the network that has already been determined and it is k_{opt}/N (k_{opt} is the optimal number of clusters in the network and N is the number of nodes in the network), r is current round number and $C_i(t)$ is an indicator function that indicates node i in the last round is cluster head or not.

Cluster head will broadcast an advertise message (ADV) to show that it is a cluster head. ADV message is a small message that contains the node ID and a small header that distinguishes this message as an ADV message.

Each non-CH node determines its own cluster for the future round by choosing CH that requires the minimum energy to communicate with its CH and the selection is based on the signal strength of received ADV messages from different CH. Usually, the nearest CH has this property for each non-CH node and it is selected as its cluster head node. If there are CH nodes with equal conditions, a node is randomly selected as CH.

After each node decided about cluster that it belongs it in the future round, should inform the respective CH. To this end, each node sends a join-request message to the intended CH using non-persistent CSMA protocol. This message also is a small message containing the node ID and a small header that distinguishes this message as a join-request message.

After receiving these messages, CHs set a TDMA schedule to coordinate data transfer in the cluster and the impossibility of collision event between nodes' data in the cluster as the center of local control and send this schedule for cluster members. As a result, it is guaranteed that no collision occurs between the messages in the cluster and also allows turning off radio components of non-CH nodes in all slots except on their own time. Thus, the consumed energy by the nodes is reduced.

Here, malicious node can mislead clustering protocol and don't let nodes join to the desirable cluster. This is done by wormhole nodes. Nodes select the nearest cluster head, the one with powerful signal, that is received by the node (its message is received earlier than other messages).The reason of this is the energy consumption of nodes becomes lower for data transfer and be prevented from relay packets by malicious nodes and the wormhole attack in this level. A malicious node can take a message and send to a node that is far away from it. In this case, the normal node selects incorrect (fake) cluster to transmit data and then, wormhole nodes achieve data between the node and the cluster head. This will prevent the wormhole attack from generating a strong signal in malicious node.

If a malicious node can convince nodes to join its desirable cluster, it can attract traffic. For this reason, the member's verification phase is done.

In members verification phase, after the clusters, cluster heads and its members have been identified; each node broadcasts a "cluster head" message to its 1-hop neighbors. Generally, the node must receive at least one message containing the cluster head ID that the requesting node is a member of the cluster. Also, the message must be received before other messages from the neighbors to the requesting node (it is used an expected time to receive). The reason is that, as shown in Fig. 3, if node i and node j are true neighbors, the overhead of the time T_{ij} from node i sends the cluster head packet to receive echo as formula 2.

$$T_{ij} = T_i^p + T_{ij}^t + T_j^p + T_{ji}^t + T_i^p \quad (2)$$

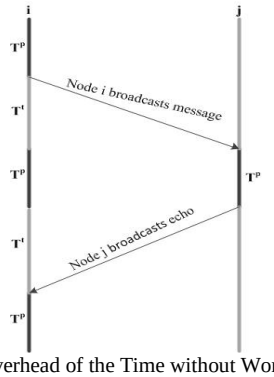

Fig. 3: The Overhead of the Time without Wormhole Attack

The notation T^p presents the time which spent processing the message and the notation T^t presents the time which spent transferring the message. In the case of wormhole attack there is the wormhole link between nodes i and j. As Fig. 4 shows, the overhead of the time T_{ij}, is given by formula 3.

$$T_{ij} = T_i^p + T_{im}^t + T_m^p + T_{mn}^t + T_n^p + T_{nj}^t + T_j^p + T_{jn}^t + T_n^p + T_{nm}^t + T_m^p + T_{mi}^t + T_i^p \quad (3)$$

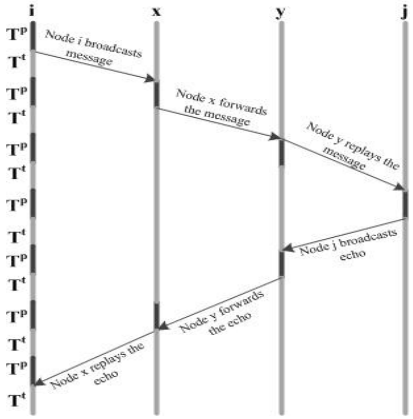

Fig. 4: The Overhead of the Time with Wormhole Attack

Actually, the time between two nodes transmission can be negligible. If the requesting node is the member of cluster head that has received the response message later than the others, the node has joined wrong cluster head and wormhole attack has occurred.

In this case, the requesting node sends a join-request message to another cluster head that has received cluster head response message from its members (and it has been received earlier than the other messages). Then, the node sends a message to the new cluster head to inform it of the existence of the wormhole nodes. Then, the cluster head sends a message to the BS and informs it from wormhole in the area.

In M-leach protocol, each cluster head is responsible for sending data to BS, but in the proposed protocol, in addition to inter cluster communication; cluster heads have intra communication with other cluster heads. In this part, the cluster head routing phase is done.

After clusters formation and cluster head verification by nodes of each cluster, the cluster head routing is done. The cluster heads use tree structures. After CHs have received messages from all nodes, then they fix the cluster boundaries and construct the spanning tree.

After certain amount of time the BS will start the tree construction by broadcasting an init_tree message to the CHs. Each CH receiving this message will store the BS information in its neighbors' table after a short period, it will send a t_accept message to the BS which contains node residual energy and its location and it will be chosen as parent for its lower level.

The parent node sends a short range broadcast message to the other cluster heads. CHs reply with the create_child message. The parent node accepts the CHs as a child if number of children is less than C_{max}. Otherwise it forwards the request to one of its child.

The threshold is set for this reason that a parent may have many children and so it can be a bottleneck and acts as a single point of failure. The imposed traffic load on the cluster head is high and it reduces the expected lifetime of the node. After that, children broadcast a parent message and act as a parent for their lower level. This procedure repeats until all CHs enter into the routing tree. The network topology which is formed by this algorithm is shown as Fig. 5.

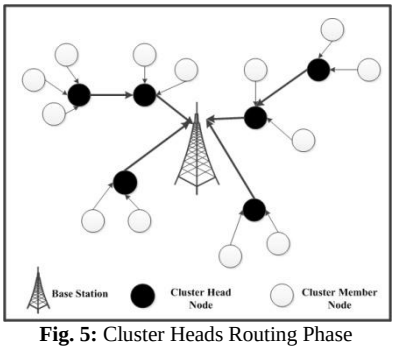

Fig. 5: Cluster Heads Routing Phase

As before, what the malicious nodes can do is preventing the tree structure from correct formation. In other words, wrong cluster heads become parent for other cluster heads that are farther than others and generally, cluster heads routing tree will not form correctly to communicate together. To prevent this, a confirmation routing is performed by the BS in cluster head routing phase. Each cluster head may receive several parent messages from other cluster heads during the route formation (tree structure).

Each cluster head records nodes ID in a table that receives routing message from them. Each two nodes that are in the range of each other, should receive routing message from each other. Upon completion of this phase, each cluster head directly sends its table to the BS.

The BS checks these tables. For example, if node B exists in the table from node A and node A does not exist in the table from node B, it is clear that the two nodes are not in range of each other and are connected by a wormhole link. Therefore the BS can find wormhole attack before sending data.
In the steady state phase, cluster head nodes collect data from their members and send it to the BS directly or through other cluster heads, after aggregation. If nodes move away from cluster head or cluster head moves away from its member nodes then other cluster head becomes suitable for member nodes and makes inefficient cluster formation. To deal with this problem, M-LEACH provides handover mechanism for nodes to switch on to a new cluster head. When nodes decide to make handoff, they send DIS-JOIN message to current cluster head and also send JOIN-REQ to new cluster head. When handoff occurs cluster heads will re- schedule the transmission pattern?
After a certain time, this round is over and the next round begins, which allows the role of cluster heads to rotate among the nodes.
One of the main advantages of this method is detection and localization of wormhole attacks before sending data. This allows reducing the destroyed, forged, or deleted data by malicious nodes. The use of efficient clustering increases the lifetime of the network and reduces energy consumption. The flowchart of the proposed method is shown in Fig. 6.

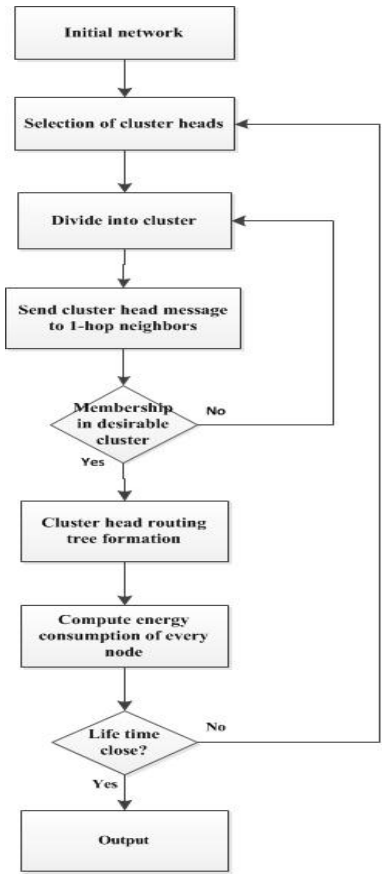

Fig. 6: The Flowchart of Proposed Method

4. Main results

NS2 simulator is used in this research. Assessment of the protocol is done in various aspects. Proposed protocol has been evaluated in terms of packet drop ratio, throughput, delay, routing overhead and energy consumption compared to a network without attack and network under attack.
To test the implementation, three simulations are used. At the first scenario, wormhole nodes are not used. In the second scenario wormhole nodes are added to the simulation. In the third scenario proposed protocol is simulated with malicious nodes in the network. Then comparison of the results is done.
To take accurate results from the simulations, UDP protocol is used. The source node keeps on sending out UDP packets, even if the malicious node drops them. Therefore, connection flow between sending node and receiving node during the simulation can be observed. Furthermore there is an opportunity to count the sent and received packets separately since the UDP connection is not lost during the simulation. Nodes travel from a random starting point to a random destination point on simulation space.
In Fig. 7, packet drop ratio is shown in a normal network, network under attack and network under attack with the proposed protocol for different times. The Average of results from the comparison diagram shows that wormhole attack

increases the drop to 90% and when the solution is implemented drop decreases to 67%. Thus it can be concluded that the packet drop decreases if there is the proposed protocol in the network.
Comparison of routing overhead and throughput are shown in Fig.8. Wormhole attack generates unnecessary routing packets in the network due to which ROH is more under attack condition and therefore, wormhole attack have higher routing overhead than normal network and the proposed protocol.
Comparison of energy consumption and delay are shown in Fig. 9.

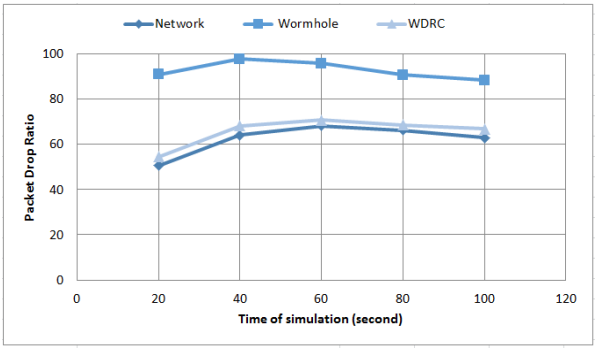

Fig. 7: Comparison of the Packet Drop Ratio. Network without Attack, the Network under Attack (Malicious Nodes) and the Network under Attack with the Proposed Protocol

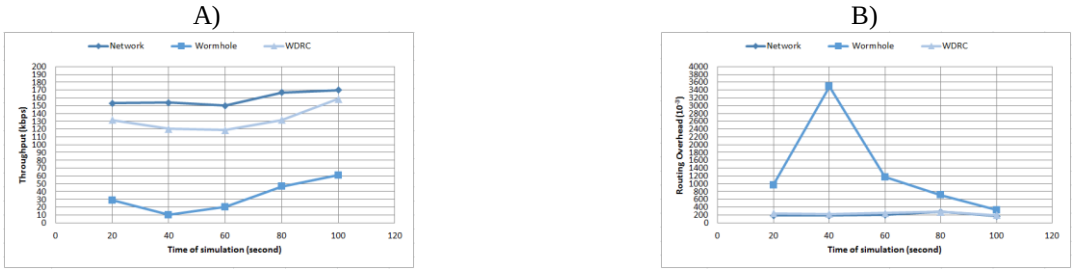

Fig. 8: A) Comparison of the Throughput. B) Comparison of the Routing Overhead. Network Without Attack, the Network Under Attack (Malicious Nodes) and the Network Under Attack with the Proposed Protocol.

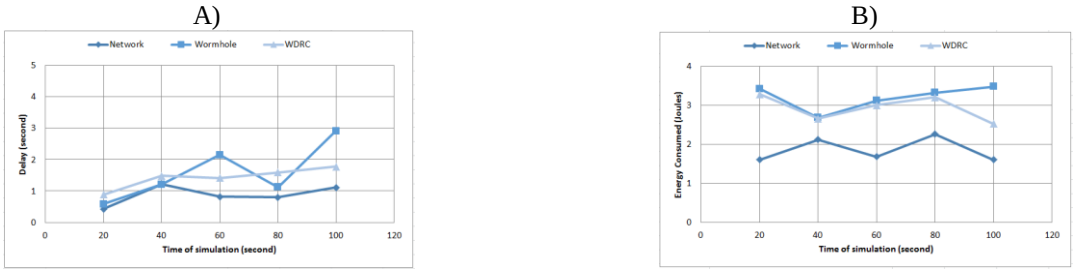

Fig. 9: A) Comparison of Delay. B) Comparison of Energy Consumption. Network without Attack, the Network under Attack (Malicious Nodes) and the Network under Attack with the Proposed Protocol.

Top charts show efficiency of the proposed protocol against wormhole attack. We can say, energy consumption is at an acceptable level but only delay metric is not optimal in the proposed protocol.

5. Conclusion

In this paper, we proposed a mechanism to detect wormhole attacks that is based on clustering consists of four phases (Setup, Members verification, Routing cluster heads and Steady state). Networks were implemented with different numbers of nodes and also malicious nodes. The obtained results from the simulator were evaluated for different network scenarios and with the proposed method in the network. The proposed protocol was evaluated in terms of packet delivery ratio, packet drop ratio, routing overhead, throughput, delay and energy consumption.
The advantage of this method is that proposed uses network broadcasting packets instead of using complex encryption or heavy computation and it is independent of network data. It is depended on the location of the nodes and their distance from the BS.
The proposed protocol can detect malicious nodes and their locations. This method is efficient for large networks. It also requires no additional hardware and it needs little processing overhead and simple calculation. As a result, the network does not consume the high energy. The proposed protocol considers limitations of wireless sensor networks and it is suitable solution to detect wormhole attacks in these networks.

The disadvantage of this approach is that the overhead of cluster formation is high in some cases (large clusters) and increases the time of detection. The delay metric (sending and receiving packets) in the protocol is not optimal, especially in large networks.

References

[1] S. Hadim and S.N. Mohamed, "Middleware challenges and approaches for wireless sensor networks", IEEE Distributed Systems, Vol. 7, No. 3, (2006) pp. 1−23. http://dx.doi.org/10.1109/MDSO.2006.19.

[2] H. Mohammadi, E.N. Oskoee, M. Afsharchi, N. Yazdani and M. Sahimi, "A percolation model of mobile ad-hoc networks", International Journal of Modern Physics C (IJMPC), Vol. 20, No. 12, (2009), pp. 1871−902. http://dx.doi.org/10.1142/S0129183109014795.

[3] M. Meghdadi, S. Ozdemir and I. Guler, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks", IETE Technical Review, - tr.ietejournals.org, Vol. 28, No. 2, (2011), pp. 89-102. http://dx.doi.org/10.4103/0256-4602.78089.

[4] Y-C Hu and A. Perrig, "A survey of secure wireless ad hoc routing", IEEE Security and Privacy", Vol. 2, No. 3, (2004,) pp. 28–39.

[5] S. Qazi, R. Raad, Y. Mu and W. Susilo, "Securing DSR against wormhole attacks in multirate ad hoc networks", Journal of Network and Computer Applications, Vol. 36, No. 2, (2013), pp. 582–592. http://dx.doi.org/10.1016/j.jnca.2012.12.019.

[6] F. Shi, W. Liu, D. Jin and J. Song, "A countermeasure against wormhole attacks in MANETs using analytical hierarchy process methodology", Electron Commer Res, Vol. 13, No 3, (2013), pp. 329-345. http://dx.doi.org/10.1007/s10660-013-9122-3.

[7] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", in the AdHoc Networks, (2003), pp. 299-302.

[8] T. Giannetsos and T. Dimitriou, "LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks", Journal of Computer and System Sciences, Vol. 80, No. 3, (2013), pp. 618-643. http://dx.doi.org/10.1016/j.jcss.2013.06.015.

[9] T. Bin, L. Qi, Y. Yi-xian, L. Dong and X. Yang, "A ranging based scheme for detecting the wormhole attack in wireless sensor networks", The Journal of China Universities of Posts and Telecommunications, Vol. 19, No. 1, (2012), pp. 6–10.