Various Techniques for Wormhole Attack Prevention in Wireless Sensor Network

Manpreet Singh[1], Usvir Kaur[2]

[1] Research Scholar, Shri Guru Granth Sahib World University, Fathegarh Sahib.,

[2] Professor, Dept of Computer Science, Shri Guru Granth Sahib World University, Fathegarh Sahib.,

Abstract:

Wireless sensor networks are remote networks and works in Ad-hoc manner. Sensor collects the information sensed by them self and send it to cluster head created in clusters. Further cluster heads use to send this information to the sink where data fetched use to complied and processed according to application used. In our research, we will propose scheme to find the energy efficient routing protocols. Sensor nodes are normally energy constrained and cannot be replaced in most cases. The need for energy efficiency in wireless sensor network is increasing considerably. This research will propose a new model to reduce the energy consumption by the sensor nodes. Proposed model distributes the energy consumption evenly among all sensor nodes to increase the life-time of the network. Most of the energy saving schemes has static nature as sensors are stationary in all. We will implement the scheme of energy efficiency for clustering based on the mobile wireless sensor nodes. Experimentation will be done with various mobility profiles to find the performance of the proposed network. Mobile devices will be move within the cluster only. Range for mobile nodes will be decided by uniform equal distance from the cluster head.

Keywords: *Wireless Sensor Nodes, Mobile Sink, Leach Protocol, Multi-hop Communication*

1. Wireless Sensor Networks

Wireless sensor networks consist of collections of small, low-powered nodes that interface or interact with the physical environment. Once deployed sensor networks are expected to operate for extended periods of time without any human intervention. [3] Substantial research effort has been directed toward increasing network lifetime by reducing radio communication, the largest source of energy drain.

Wireless sensor networks (WSN) are networks usually comprised of a large number of nodes with sensing and routing capabilities [1]. Multi-hop routing is usually implemented for the transport of the sensed data to special data collection nodes (the sinks). Among the challenges posed by the problem of data delivery to the sinks one that has recently received considerable attention concerns the minimization of the node energy consumption for increasing the overall network lifetime. Previous research aimed toward this major goal has been prevalently concerned with developing techniques for topology control [1], energy efficient MAC and routing.

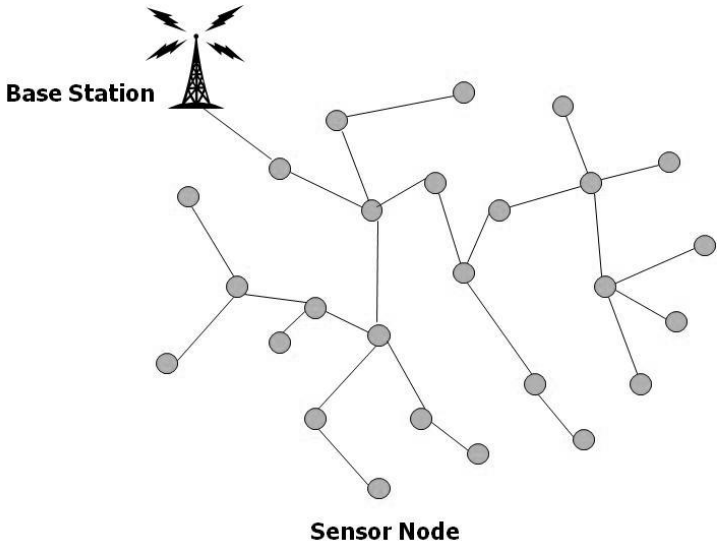

Fig. 1 Sensor nodes exchange data to build a global view of the monitored region [7]

Most of the considered scenarios deal with sensor nodes that do not move and are un-replaceable, where the sensed data have to be delivered to the sinks that are static as well.

A trend of the research on data dissemination in WSNs has recently started where the mobility of some of the nodes is exploited to facilitate the delivery of the sensed data to the sinks. Considering mobility as "a blessing" rather than a curse to network performance has been widely discussed for general ad hoc networks in different contexts [2]. The primary objective of these works is to deliver messages in disconnected ad hoc networks and to improve network throughput. The work [8] explores the possibility of using the coordinated motion of a small part of users in the network to achieve efficient communication between two other mobile nodes.

Generally Adhoc on demand protocol used in wireless sensor networks for routing purposes. On demand routing process maintain information about routing in very small intent because information use to fetch on demand. Our experimentation will base on attacks prevention in on demand routing protocols in wireless sensor network.

2. Attacks in Sensor Network

The open nature of the wireless communication channels, the lack of infrastructure, the fast deployment practices, and the hostile environments where they may be deployed, make them vulnerable to a wide range of security attacks. The attacks such as [5]

1) Spoofed, altered, or replayed routing information
2) Selective forwarding
3) Sinkhole attacks
4) Sybil attacks
5) Wormholes
6) HELLO flood attacks

Spoofed, altered, or replayed routing information

The most direct attack against a routing protocol is to target the routing information exchanged between nodes. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.[1]

Selective forwarding

Multi-hop networks are often based on the assumption that participating nodes will faithfully forward receive messages. In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet. [3]

Sinkhole attacks

In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the centre. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. [4][5].

HELLO flood attack

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. [3]

Wormhole attack

In the wormhole attack, an attacker tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other

nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker.

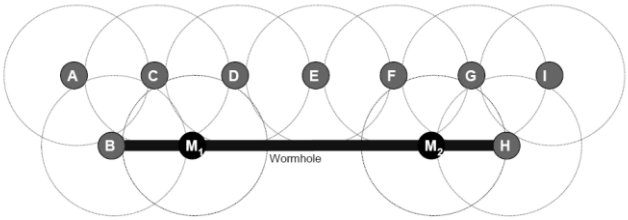

Fig. 2: Two or more malicious nodes collaborate in setting up a shortcut link between each other [7]

An attacker situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An attacker could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the attacker on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through if alternate routes are significantly less attractive. This will most likely always be the case when the endpoint of the wormhole is relatively far from a base station [4].

3. Wormhole Prevention Phase by key Distribution

In commonly used Dynamic Routing Algorithms, Route Request (RREQ) packet is broadcasted by the source node. All nodes receiving this packet broadcast it further until it reaches to the destination. As shown in the Fig. 3, nodes A and O are source and destination nodes respectively. Node A is broadcasting RREQ packet. [8]

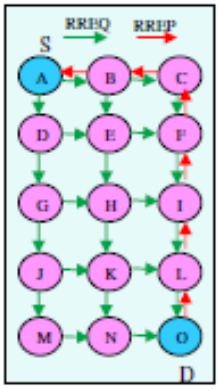

Fig. 3: Transmission of RREQ and RREP Messages

On receiving this packet, node O forwards Route Reply (RREP) packet for the path from which it obtains the first RREQ packet.

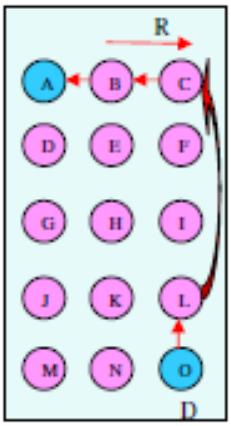

Fig.4: Transmission of RREP Message via Wormhole Link

Let use consider a case where a wormhole link is present between node C and node L. When RREQ is received by node C, it will be diverted to node L directly via the established out-of band wormhole link. In this case, RREP packet follows the path shown in fig 4. For wormhole prevention, each node is supposed to store the detail of each and every RREP packet it forwards. On receiving RREP, its validity is tested through a check phase which is started with broadcasting of Probe message and its corresponding Probe_Ack_Tag value. For various possible cases the sequence is explained further. [8]

4. Distributed Approach to Mitigate Wormhole Attack

In order to mitigate effect of wormhole attack in wireless sensor network, a distributed neighbor discovery approach has been proposed. There are some criteria to determine whether wormhole attack is performing in the network or not. For example some methods use statistical approach. They find dramatic changes in the certain statistical patterns and then decide on existence of wormhole in the network. Longer propagation can be another symptom of wormhole existence. Additionally we can determine the existence of wormhole in the network by checking the parameters such as bigger transmission range than that of normal condition, and previous node is not a neighbor as well.

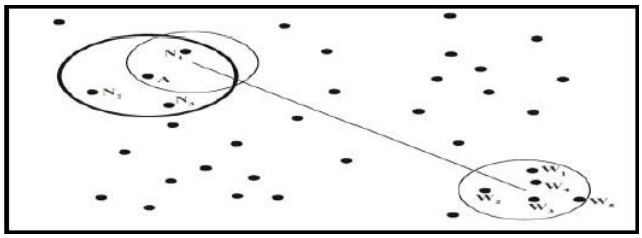

Fig. 5: Illustration of the sensor network [11]

The proposed method is based on the fact that mentioned wormhole data comes from unauthorized and illegal neighbors. In order to illustrate the idea of the proposed neighbor discovery technique, consider Fig. 6 presented at below. This figure illustrates of network with 12 nodes.

Consider tow nodes ‘A’ and ‘B’. The actual neighbors of node ‘A’ are ‘A1’ and ‘A2’ and the real neighbor of node ‘B’ are ‘B1’ and ‘B2’. This means that node ‘A’ receives information only form nodes ‘A1’ and ‘A2’ and nodes ‘B1’ and ‘B2’ only send data to node ‘B’. As it is shown in the Figure 5, node ‘A’ is connected to node ‘B’ through the wormhole. Therefore node ‘A’ can also receive data from node ‘B’ and vice versa.

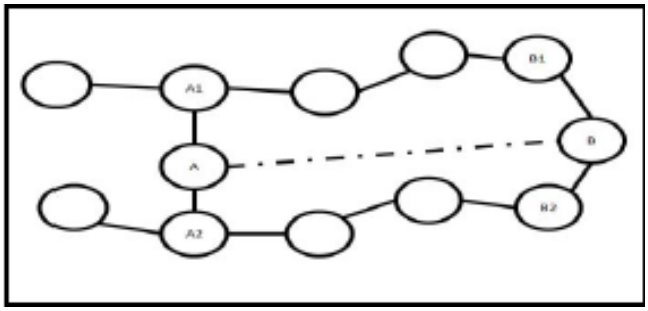

Fig. 6: Illustration of Network Affected with Wormhole

The problem of wormhole attack will be solved if the receiving node can determine whether arrival data comes from actual neighbor or not. Therefore in order to mitigate the effect of passive wormhole attack which attacker is not belong to the network and does not use the sensor devices to receive and forward the data through the wormhole tunnel, neighbor discovery protocol has been proposed.

5. Wormhole Detection by Synchronization

The approach proposed here mainly focuses on the number of sent and received packets, from and to each of the node in the network by checking the validity of the gathered data, it can identify whether the network is attacked by the wormhole nodes or not. Statistics about the number of sent and received packets is maintained by storing two tables at each node, namely Sent_Packets and Rcvd_Packets. Both the tables have one entry for each of its one-hop neighbor and on counter value initialized with zero. When a packet is sent by a node, corresponding counter value for the node to which it is sent is incremented in Sent_Packets. Similarly, Rcvd Packets keeps track of number of received packets from each of the neighbor node. Let us consider a case, where node 2 has four neighbors: node 1,3,4 and 5. So node 2 has four entries, one for each neighbor node. Each entry stores a counter with initial value zero, along with the node ill. For this case, when node 2 sends a packet to node 5, corresponding entry in Sent_Packets table is incremented provided the packet sent by node 2 is not destined for node 5. Exactly opposite when node 2 receives

a packet from node 5, the corresponding entry in Rcvd_Packets of node 2 is incremented with the condition that the packet might not have been originated by the node 5. The conditional increment and decrement operations are required to focus only to the kind of send and receive operations, where the concerned node is expected to forward the packet to any of the one-hop neighbor. Infolmation maintained by all the nodes is then sent to the base station at regular interval where it is analyzed. Considering the case for node 2, one hop neighbors of node 2 give values of PSi. Z where PS□ 2 is number of packets sent by node i to node 2, and i is one of the neighbor node of node 2. The approach proposed here mainly focuses on the number of sent and received packets, from and to each of the node in the network by checking the validity of the gathered data, it can identify whether the network is attacked by the wormhole nodes or not. Statistics about the number of sent and received packets is maintained by storing two tables at each node, namely Sent_Packets and Rcvd_Packets. Both the tables have one entry for each of its one-hop neighbor and on counter value initialized with zero. When a packet is sent by a node, corresponding counter value for the node to which it is sent is incremented in Sent_Packets. Similarly, Rcvd Packets keeps track of number of received packets from each of the neighbor node. Let us consider a case, where node 2 has four neighbors: node 1,3,4 and 5. So node 2 has four entries, one for each neighbor node. Each entry stores a counter with initial value zero, along with the node ill. For this case, when node 2 sends a packet to node 5, corresponding entry in Sent_Packets table is incremented provided the packet sent by node 2 is not destined for node 5. Exactly opposite when node 2 receives a packet from node 5, the corresponding entry in Rcvd_Packets of node 2 is incremented with the condition that the packet might not have been originated by the node 5. The conditional increment and decrement operations are required to focus only to the kind of send and receive operations, where the concerned node is expected to forward the packet to any of the one-hop neighbor. Infolmation maintained by all the nodes is then sent to the base station at regular interval where it is analyzed. Considering the case for node 2, one hop neighbors of node 2 give values of PSi. Z where PS□ 2 is number of packets sent by node i to node 2, and i is one of the neighbor node of node 2.

6. Conclusion

This paper explains the concept of wormhole elimination schemes by various techniques. Mainly focused on key distribution and the synchronization process to avoid wormhole attacks in wireless sensor network and mobile adhoc network. In our nearby experimentation, we are working on elimination of wormhole attack by implementing traffic monitored scheme.

References

[1] Z. Maria Wang, Stefano Basagni, Emanuel Melachrinoudis and Chiara Petrioli, ‘‘Exploiting Sink Mobility for Maximizing Sensor Networks Lifetime’’, Proceedings of the 38th Hawaii International Conference on System Sciences, IEEE Computer Society, 2005.

[2] E. H. Callaway, Jr,” Wireless Sensor Networks: Architectures and Protocols”, Boca Raton, FL: Auerbach Publications, August 2003.

[3] Thanos Stathopoulos, Rahul Kapur, Deborah Estrin, “Application-Based Collision Avoidance in Wireless Sensor Networks”, Conference of Computer society, pp. 335-343, July-December 2005.

[4] Kuldeep Kaur, Vinod Kumar & Upinderpal Singh, “Detection of Wormhole Attack in Wireless Sensor Networks,” IRNet Transactions on Computer Science and Engineering, 2011.

[5] Guiyi Wei Xueli Wang "Detecting Wormhole Attacks Using Probabilistic Routing and Redundancy Transmission". WASE International Conference on Information Engineering, pp. 251-254, 2010.

[6] Dhara Buch and Devesh linwala, "Detection Of Wormhole Attacks In Wireless Sensor Network", Proc. of Int. Con! on Advances in Recent Technologies in Communication and Computing, IEEE, 2011.

[7] Lukman Sharif and Munir Ahmed," The Wormhole Routing Attack in Wireless Sensor Networks (WSN)", Journal of Information Processing Systems, pp. 345-347, Vol.6, Issue.2, June 2010.

[8] Dhara Buch and Devesh Jinwala" Prevention of Wormhole Attack In Wireless Sensor Network ", International Journal of Network Security & Its Applications (IJNSA), Vol.3, Issue.5, Sep 2011.

[9] Dezun Dong, Mo Li, Yunhao Liu And Xiangke Liao, "Connectivity-Based Wormhole Detection in Ubiquitous Sensor Networks", Journal Of Information Science And Engineering Vol.27, pp. 65-78, 2011.

[10] Ali Modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni, Naghmeh Niknejad," Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", Wireless Engineering and Technology, IEEE, pp. 142-151, Vol. 3, 2012.

[11] Lee, Gunhee, Kim, Dong-kyoo and Seo, Jungtaek.,"An approach to mitigate wormhole attack in wireless ad hoc network", 2008, International conference on information security and assurance. pp. 220 - 225.