ISSN:0975-9646

Cluster Based Secure WSN against the Blackhole and Grayhole Attack

Ojashvi Shivwanshi, Rahul Patel, Preetika Saxena

CSE-AITR Indore, RGTU Bhopal
Indore Bypass Road, Mangiliya Square,
Indore, M.P., India

***Abstract*—The wireless technology is growing continuously and a number of applications are developed using the wireless communication methodologies. Among them the wireless sensor network is one of the most rapidly applicable network applications. The sensor nodes are configured in critical situations therefore the efficiency is major expectation in this network. In addition of that the network is simulating the ad hoc behaviour therefore the security is also a critical aspect of the network. in order to improve the network for performance and security a number of solutions are available but there are fewer solutions are exist that providing both the security as well as performance. Therefore in this presented work a cryptographic cluster based communication technique is proposed for preventing the network from attackers. In addition of that the clustering schemes are help to improve the performance of network in most optimum manners. For securing the network the cluster network includes the Blackhole and Grayhole attack for detection and prevention. The implementation of the proposed secure technique is performed using the AODV routing in NS2 (network simulator 2) environment.**

***Keywords*— WSN, Blackhole, Grayhole, AODV, survey, review**

I. INTRODUCTION

A wireless sensor network is a distributed real-time system [1]. The network is changing self-according to the need of application therefore assumptions underlying earlier work has changed dramatically. Most of the distributed systems following assumption like the systems are wired. But the presented work is focused on the wireless sensor networks where the powers are unlimited, not works on real-time, and also having fixed set of resources. These systems are having two kinds of behaviour first statically establishes and following the completely ad-hoc manner of communication. In ad hoc manner the mobility and changing topology is property of network. On the other hand the network needs an efficient manner of consuming the resources.

Due to the ad hoc nature of the network that is a kind of adoptive network technology. In network the wireless nodes any time join or leave the network. By which any malicious node can also join the network and harm the privacy and security of the network. Therefore in this network not only the performance is key objective of network design the security aspects are also considered during the network design. Due to analysis of the network that is observed the network is more rapidly affected by the routing based attack deployment among Blackhole, wormhole and the Grayhole attack are much frequent attacks in network routing. Therefore the proposed work is concentrated on finding solution for the Blackhole and wormhole attack.

II. LITERATURE SURVEY

This section provides the information about the background technology and the attack deployment technique, this may help in understanding the functional aspects of the attackers.

A. Blackhole Attack

In Black hole attack, using routing protocol to an attacker advertises itself as the shortest path to the target device [2]. An attacker watches the routes request in a flooding based routing protocol. When the attacker receives an appeal for a route to the target node, it forms a respond involving of really short route. If the mischievous respond reaches the initiating node before the reply from the genuine node, a fake route gets created. Once the malicious device joins the network itself among the communicating nodes, it is bright to do anything with the packets passing through them. It can crash the packets between them to perform a denial-of-service attack, or on the other hand use its position over the route is the first step of man-in-the-middle attack [3]. The black hole attack is a well-known security issue in WSN. The intruders develop the loophole to deploy their malicious activities because the route detection process is necessary and predictable. Many researchers have conducted different detection techniques to propose different types of detection schemes [4].

For example, in Figure 1, source node S wants to send data packets to destination node D and initiates the route detection process. Suppose that device 2 is a malicious device and it claims that it has a route to the destination whenever it receives route request packets, and straight away sends the reaction to node S. If the reply from the malicious node 2 influences firstly to node S, then node S considers that route detection is finished, than S ignores all other replies and starts to send data packets to node 2. As an outcome, all packets through the malicious node is consumed or lost.

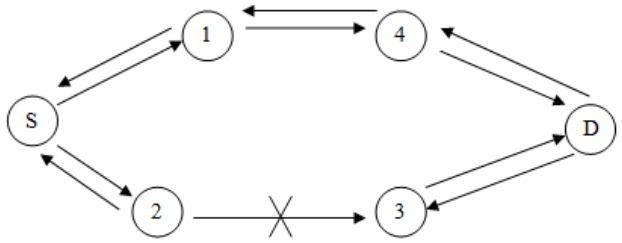

Figure 1 Black hole attack

B. Grayhole Attack

In AODV protocol, every mobile node maintains a routing table that stores the next hop node information for a route to a destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if such a route is available in its routing table. Otherwise, the node initiates a route discovery process by broadcasting a Route Request (RREQ) message to its neighbors. On receiving a RREQ message, the intermediate nodes update their routing tables for a reverse route to the source node. All the receiving nodes that do not have a route to the destination node broadcast the RREQ packet to their neighbors. Intermediate nodes increment the hop count before forwarding the RREQ. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to the destination.

We now describe the Grayhole attack on WSN. The Grayhole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainty [5]. A Grayhole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Grayhole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A Grayhole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.

III. Problem Domain

The proposed work is intended to find the efficient and effective solution for the Blackhole and Grayhole attack conditions in the wireless sensor network. There are a number of individual solutions are exist for preventing and attack in network but there are two few solutions are available for secure the network from both the attacks using the same techniques. Therefore the proposed work is intended to find a common solution for both the issues in network.

IV. Solution Domain

The proposed solution incorporates the cluster based solution for recovering the network from the Blackhole and Grayhole attack. The proposed solution works in three major steps in the following manner.

1. **Cluster formation**

To improve the performance for the mobile wireless sensor networks that is required to select effective parameters to develop better resource preservation methodology. In order to improve the technique a weighted clustering based routing technique is proposed. The utilized parameters are defined as follows.

Connectivity: In this network the nodes are said to be connected if the nodes are in radio range of a node. Thus Maximum numbers of nodes are in connected through this node causes the more serving capability.

Remain Energy: The network devices in mobile WSN are created with limited energy. But if a node loss their energy frequently then the node is not functioning as required. Thus remain energy is an essential parameter for clustering, that will be computed using the below given formula.

$$E = initial\ energy - last\ energy$$

If the node energy is regulated according to the need thus the performance of network can be improvable in terms of energy consumption.

Mobility: Another property of node in ad hoc network is mobility. Nodes are frequently moving from one place to other in this network randomly. The low mobile nodes are able to form more stable clusters. Because these nodes are connected with a long time as compared to different mobility nodes, thus node mobility can be computed using the following formula.

$$M = \frac{1}{T}\sum_{t=1}^{T}\sqrt{(X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2}$$

Buffer length: in network and socket programming the nodes are first accept the data using the buffer and for collecting information from the network that again utilizes the buffer. If the allocated buffer size of the node is consumed by the node that means a node in a high processing load or it suffers from the congestion problems thus the node which having less filled buffer can serve better as compared to filled buffer node.

The estimated all the parameters are defined in different scales therefore the normalization process is required for combining these parameters. Therefore a weight is required to compute by which all the parameters are scaled on a similar scale. To compute weights also help to find the optimum node in network, thus a list of efficient nodes are created using the calculated weights.

$$W = w_1 * c + w_2 * E + w_3 * M + w_4 * B$$

In this weight calculation is performed by scaling the node performance parameters into a similar scale therefore $w_1, w_2, \ldots$ are providing the factors on with the nodes parameters are scaled. For constructing these factors the sum of these factors is required to be 1 and the distribution of these weights are between 0-1.

2. **Detection of secure route**

In order to find the Blackhole and Grayhole attacker nodes the initial working of the network is find as the normal AODV. The AODV based route discovery is implemented first to find out the best path and to send data to all destination nodes. In addition of that an extra information packets contain the info of packets IDs and time of receiving are transmitted, this packet now send to the neighbour nodes if there is no attack destination node receive the original packet of that ID and send a confirm packet to the sender in reverse order. If sender node not receive confirmation packet till 5 sent packets in a predefined time than, now CH check every info packet that node whose next hop not send then this packet mark as malicious node and remove from the path after finding the attacker node.

3. **Cryptographic data exchange**

For improving the security more effectively the AES algorithm is used encrypt the data and DH key exchange mechanism is used for preserving the key exchange during the data exchange.

V. CONCLUSION

In this given paper a review on the exiting technology and the recently made development on the security of wireless sensor network will be observed. In addition of that a combined solution against the Blackhole and Grayhole is proposed. The proposed approach first obtain the most promising path among the source and destination and then the cryptographic technique is used to secure communication of the network. The proposed concept is further implemented using the NS2 simulation environment and with the help of AODV routing protocol. Additionally the implementation based performance analysis is also reported in the future work.

REFERENCE

[1] Mo Li, Zhenjiang Li, and Athanasios V. Vasilakos, "A Survey on Topology Control in Wireless Sensor Networks: Taxonomy, Comparative Study, and Open Issues", Proceedings of the IEEE | Vol. 101, No. 12, December 2013

[2] Shree Om and Mohammad Talib, “Wireless Ad-hoc Network under Black-hole Attack”, 2011 ISSN 2225-658X.

[3] Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil, “Black Hole Attack Injection in Ad hoc Networks”.

[4] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, Tseng et al. Human-centric Computing and Information Sciences 2011.

[5] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar, “A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks”, 1-4244-0983-7/07/$25.00 ©2007 IEEE