Abstract - Securing the routing procedure is an important issue in wireless sensor network. Previously, some works on the trust based dynamic source routing protocol (DSR) are used for that. In this paper, to improve the quality of this procedure a modified design of trust based dynamic source routing protocol is proposed. Here, first find out trust values of all the nodes by the trust model. In the existing trust models each node’s trust table contains trust value of its neighbors. But in this proposed solution each node’s trust table contain only its own value. So this will reduce the transmission overhead over the network. Then DSR is used for routing packets through the nodes. The nodes with trust value higher than or equal to the threshold will select for the routing path. A CRC field also added in the route replay message in the DSR for ensuring integrity. This will helps to improve the efficiency of routing procedure.


I. INTRODUCTION

Wireless sensor network consist of spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, motion, vibration and pressure. Security [1] has an important role in the routing procedure. A wide variety of security attacks such as black-hole and grey-hole attacks address the routing procedure. In the black hole and grey-hole attacks the selfish nodes are refused to forward all or part the traffic received from its neighbors. These kinds of attacks can be avoided by using the proposed solution. In the trust model each node establishes trust relationship with each other and base their routing decisions not only on pure or geographical information but also on their expectation that their neighbors will sincerely cooperate. Trust is the confidence of a node ki that a node kj will perform as is expected. The method for obtaining trust information defining each node’s trustworthiness are termed as trust models .The concept is to create on each sensor a trust repository table which will maintain and handle the information. Trust values are computed between 0 and 1. All these schemes are aim to improve the security and thus to increase the throughput. DSR is a simple and efficient protocol which is designed specifically for multi-hop wireless communication. Using DSR the network is self-organizing and self-configuring. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR protocol. Since the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing.

Figure .1 Wireless sensor networks

A modified trust based dynamic source routing protocol is used to find out the secure routing path for packet transmission. In this, first find out the trust values of all nodes in the transmission range. Then DSR protocol is used for routing discovery and route maintenance on these nodes. This will reduce chance of selecting attacker nodes in the routing path.

II. RELATED WORKS

A secure routing protocol is used in wireless sensor networks for routing selection [2] [3].There is many trust based models [4] [5] [6] are used for routing procedure. In Some previous approaches the trust establishment is realized in a centralized manner. All these methods are used different parameters as metrics for calculating the trust value. The Dynamic source routing protocol [7] is used for route discovery in wireless sensor networks. There is one trust based DSR is already proposed. In this the trust value of all the nodes are broadcasted over the network. This will increase the transmission overhead and delay of this model. The existing approach [8] used in the proposed integrated design, the trust model is a fully distributed scheme. This trust model is suitable for the ad-hoc and wireless sensor networks. The concept is to create on each sensor a trust table which will maintain and handle trust and reputation information about each neighboring node. In the trust table values regarding a number of events are stored. Here the aspects to monitor are packet forwarding, network layer ACK, confidentiality, integrity, authentication, remaining energy.

© 2011 ACEEE
DOI: 02.CEMC.2011.01. 534
Then based on these values, an overall cost function is calculated and drives the selection of the forwarding node. The DSR protocol [7] used in the proposed method has mainly two functions. Route discovery and route maintenance. Route discovery and route maintenance each operate on demand. In particular, unlike other protocols, DSR requires no periodic packets of any kind at any level within the network. Figure 2 illustrates an example of route discovery. In this node A send a packet to a node D. To initiate the route discovery, A transmit a route request as a single local broadcast, which is received by all the nodes within the transmission range. Each route request identifies the sender and destination. Also contain the unique request id, record listing of address of the intermediate nodes through which particular copy of the route message is again forwarded.

When a node receives the route request, if it is the target, it then returns a route reply message to the sender, giving the copy of the route record from the route request. Some attacker nodes in the path will modify that message. This will harm the integrity of the message. To overcome this problem a solution is used in the proposed solution. When the sender receives a route reply from destination, it caches this route in its route cache for use in sending subsequent packets to the destination. The sending node will have a send buffer which contains a copy of each packet that cannot be transmitted by this node because it does not have a source route to the packet destination.

In Figure 3 the node C is unable to forward the packet to the destination D, then C return an error message to A stating that the link from C to D is broken. Then A is retransmitting that packet through another path. The main disadvantage of the trust model is that there is no specific protocol for routing procedure. And in the case of DSR, during the routing some nodes in the routing path will slow down or refused to forward the packet. To find out such nodes trust based dynamic source routing is used. This will provide more security. Previously, there is one available work on the trust based dynamic source routing protocol. Here the trust value is calculated and drives the selection of the forwarding node. The main idea is to create on each sensor a trust repository which contains only the information about its own trust value. Broadcasting of the trust value is avoided here to reduce the delay. In this, each node calculates its own trust value. A threshold is set for the trust value. The nodes with trust value less than the threshold will considered as attacker and nodes with value greater than or equal to threshold is considered as trustable. The attacker nodes are avoided during the routing procedure. The behavior aspects to monitor the trust calculation are packet forwarding, network layer ACK, confidentiality, integrity, authentication, remaining energy. The trust value calculated by the following equation.

\[ T = \frac{S}{S+F} \]  \hspace{1cm} (1)

Where T denotes the trust value. S and F are the success and failed co-operations successively. To perform routing decisions, a weighted cost function is calculated which incorporates the trust information as well as the location information. The weighted function is as follows.

\[ W(T) \times T + W(D) \times D \]  \hspace{1cm} (2)

Where W(T) and W(D) are the weights applied to the trust value and distance respectively and D is the distance. Using (2) calculates the trust value of each node. The nodes with trust value greater than the threshold will selected for routing. Then apply DSR protocol. The DSR protocol mainly contains two mechanisms. Route discovery is the mechanism by which a node S wants to send a packet to the destination node D. For that first obtain a source route to D. The route discovery is applicable is used only when S attempts to send a packet to D and does not already know a route to D. Route maintenance indicates a source route is broken, S can attempt to use any other trustable node in the path to the D.

III. A MODIFIED TRUST BASED DYNAMIC SOURCE ROUTING PROTOCOL

It is the improved integrated design of trust model and DSR. The trust model is used to find out the trust value of all nodes in the routing path. The DSR is used as the routing protocol for routing the packets through the nodes. The trust value of each node is calculated by the trust model. The main idea is to create on each sensor a trust repository which contains only the information about its own trust value. Broadcasting of the trust value is avoided here to reduce the delay. In this, each node calculates its own trust value. A threshold is set for the trust value. The nodes with trust value less than the threshold will considered as attacker and nodes with value greater than or equal to threshold is considered as trustable. The attacker nodes are avoided during the routing procedure. The behavior aspects to monitor the trust calculation are packet forwarding, network layer ACK, confidentiality, integrity, authentication, remaining energy. The trust value calculated by the following equation.

\[ T = \frac{S}{S+F} \]  \hspace{1cm} (1)

Where T denotes the trust value. S and F are the success and failed co-operations successively. To perform routing decisions, a weighted cost function is calculated which incorporates the trust information as well as the location information. The weighted function is as follows.

\[ W(T) \times T + W(D) \times D \]  \hspace{1cm} (2)

Where W(T) and W(D) are the weights applied to the trust value and distance respectively and D is the distance. Using (2) calculates the trust value of each node. The nodes with trust value greater than the threshold will selected for routing. Then apply DSR protocol. The DSR protocol mainly contains two mechanisms. Route discovery is the mechanism by which a node S wants to send a packet to the destination node D. For that first obtain a source route to D. The route discovery is applicable is used only when S attempts to send a packet to D and does not already know a route to D. Route maintenance indicates a source route is broken, S can attempt to use any other trustable node in the path to the D.

1. Find out the trust value of all the nodes based on Packet forwarding
   Network layer acknowledgement
   Confidentiality, integrity etc

2. If a node want to send a data
   2.1 First send a route request to all other nodes in the wireless coverage area
   2.2 Intermediate nodes are again forwarded the request with id, record which contain list of nodes and its trust value

3. The nodes with trust value less than threshold refused to forward the request
4. The node which sends the request will take another path
5. If the request reaches the destination it returns a route reply to the source

Figure 4 Pseudo code for modified trust based DSR protocol
Poster Paper

The working is as follows. The node A wants to send a packet to node D. For that, the sender A broadcasts a route request message to all the nodes in its wireless range. The node B receives it and reforwarded. Finally, it reaches the destination. In the trust-based DSR in addition to the ID and the record which contain the list of nodes, each node sends its trust value (T). Each node has its own trust table and its trust value is stored in it. The nodes with lower trust values are avoided from the routing path. When the target node receives the route request, it sends back a route reply which contains the list of route record, trust value, and a CRC field. The CRC field is used for providing integrity. This will prevent the modifications of route reply message. If A receives two route replies (two different paths) from D, then A can select best path (the path have less hopes). In Figure 5 destination D sends a reply to A with the routing path namely A, B, E, F, D. Here C is the attacker node and its trust value is less than the threshold. So C will refuse to forward the route request to D. So D will send back the routing path A, B, E, F, D. Route maintenance is exactly the same as that of the existing DSR protocol. If a node unable to forward a packet then it will send an error message. Then that packet is retransmitted through another path. The main advantage of the trust based dynamic source routing protocol in wireless sensor network is the detection of routing attacks such as black hole and grey-hole attack. Some attacker nodes will place along the routing path. In the case of DSR, only after sending the packet to the attacker node the sender can understand that that node is an attacker node. But in the case of trust-based DSR, the trust value in the trust table will give the information about whether it is an attacker or not.

DISCUSSIONS

Trust-based Dynamic Source Routing Protocol is mainly used for securing the routing procedure. In this paper, a modified trust-based DSR is used for detecting the black hole and grey hole attacks. Here each node’s trust table contains only its own trust value. In the current model, after calculating the trust value each node broadcast its trust value. So it causes transmission overhead in the network. In the proposed model, there is no need for broadcasting the trust values over the network. In addition to this for ensuring integrity CRC field is also used.

CONCLUSIONS

Previously, there is an available work on the integrated design of trust model and dynamic source routing protocol. The main aim of trust-based DSR is to provide security during the routing procedure. In this, the trust model is used to find out the trust value of each node. Here each node’s trust table contains only its own trust value. After finding the trust values of each node DSR is used for selecting the routing path. The nodes with trust value less than the threshold are refused to forward the packet. These nodes are avoided from the routing procedure by checking its trust value in the trust table. Also, the route reply contains a CRC field, which will provide integrity. So the improved trust-based DSR provide more security in the case of routing attacks detection in wireless sensor networks.

REFERENCES