SECURING ROUTE DISCOVERY IN MAODV FOR WIRELESS SENSOR NETWORKS

R.Shyamala*, Dr.S.Valli**
* Lecturer, Department of Computer Science and Engineering, University College of Engineering, Tindivanam. vasuchaaru@yahoo.com
** Assistant Professor, Department of Computer Science and Engineering, Anna University, Chennai-25. valli@annauniv.edu

ABSTRACT
The deployment of sensor networks for security and safety related environments requires securing communication primitives such as broadcast, multicast and point to point communication. Recent research shows that multicast provides high energy saving in IP supported wireless sensor networks (WSN). In this work, we investigate how to secure route discovery of the Multicast Ad-hoc on Demand Distance Vector (MAODV) protocol for WSNs. For the ad-hoc networks ARIADNE, SEAD, ARAN are some of the solutions, which cannot be directly applied to energy constrained WSNs. Here, we propose a secure route discovery of MAODV based on TESLA and one-way hash function. We have simulated our work using NS-2. The performance of the secured MAODV and the unsecured MAODV is compared.

Keywords – MAODV, TESLA, Multicast, packet delivery ratio.

1 INTRODUCTION
Wireless sensor networks [1] (WSN) consist of a large set of multi-functional, low cost, wirelessly networked sensor nodes. These sensor nodes have control components and communication functionality. Sensor nodes cooperate with each other and are deployed in environment monitoring, habitat monitoring, healthcare, home automation, traffic control and industrial system automation. Recent work [2] [26][25] shows that rather than broadcast, multicast in sensor network saves power. Among various routing protocols [11] MAODV has a very good performance.

For the application of MAODV, a platform that supports IP functionality in WSNs is required. Since sensor networks have power consumption restriction, it is too complex to apply the full TCP/IP protocol stack with IPV6 functionality to them. The authors [8][25] describe a mechanism, which enables IP addressing in sensor nodes in a 4G-environment. The IETE group has also created, LOWPANWG, which addresses IPV6 functionality for Personnel Area Networks (PAN) including WSNs. The SICS research group developed a new microprocessor, a WSN-oriented operating system called Contiki [7], which describes IP connectivity. The authors [25] developed a test bed with IP and multicast support in WSNs and concluded that it is feasible to apply source specific multicast to WSNs.

In sensor networks, adverse nodes can freely join the network, listen to and/or interfere with network traffic, which leads to network failures. So, it is necessary to design a security mechanism that can prevent attacks by insiders or outsiders for the tree based routing protocol, namely MAODV.

2 RELATED WORK
Recently, several works have addressed securing unicast routing protocols for ad-hoc networks. ARIADNE [15], Secure Efficient Ad hoc Distance vector (SEAD) [14], Authenticated Routing for Ad hoc Networks (ARAN) [18], Secure Ad hoc On-demand Distance Vector (SAODV)[9], and Byzantine-Resilient Secure Multicast Routing in Multi-hop Wireless Networks (BSMR) [6] are the works, which secure routing protocol.

ARIADNE [15] is based on Dynamic Source Routing (DSR); it describes end-to-end security for ad-hoc network routing. It makes use of the message authentication code (MAC) to authenticate routing table entries. It requires clock synchronization in the network since the security of DSR is based on TESLA. SEAD [14] secures the Destination-Sequenced Distance-Vector (DSDV) routing protocol and provides authentication using TESLA. It requires a shared secret key between each pair of nodes. ARAN [18] uses limited time certificates. So, it requires a trusted certificate authority. This protocol increases latency and discovers optimal shortest paths. SAODV [9] combines digital signature and hash chain and gives a secure Ad hoc On-demand Distance Vector (AODV). It splits the message into mutable and non-mutable fields. Cryptographic signatures are used to authenticate non-mutable fields. A One-way hash chain is created for every route discovery process to secure a hop count field, a mutable field of the AODV message. This protocol requires a key management mechanism. In any on-demand routing protocol, route discovery plays an important role. So, we consider how to secure route discovery with minimal cryptographic primitives, such as hash function and symmetric encryption for wireless sensor networks.

The rest of the paper is organized as follows; section 3 describes the network model and system assumption used in the implementation. Section 4 describes how to secure route discovery of MAODV. Simulation results are given in section 5 and section 6 concludes the paper and suggests future work.

3 NETWORK MODEL AND SYSTEM ASSUMPTION

We assume that a network has a central base station and sensor nodes are densely deployed. The base station has abundant computation resources. The base station has a private/public key pair; the public key of the base station is known to all the sensor nodes. For our system we require a trusted key distribution center (KDC). The base station acts as the KDC. It is trustworthy and cannot be compromised. The sensor nodes communicate using unreliable radio links. The nodes in the sensor network are resource constrained. Each node has a unique ID. The nodes communicate with each other by multihops. Since we use the TESLA-based certificate for secure route discovery, all the nodes have loosely synchronized clocks. The clock difference between any two nodes does not exceed the error rate (Δ). All the nodes know the value of Δ. The time synchronization is maintained by the hardware. The network links are bi-directional.

We assume that an attacker attempts to tamper with some links to reduce routing information to its neighbor. An intruder can jam outgoing packets. An attacker may be a compromised node. If so, it will make use of all the cryptographic keys and it may cooperate with other attackers. We make no assumption on the number of intruders, their location and their radio range.

3.1 Tesla

Perring et al [23] present an efficient source authentication technique called TESLA. It uses pure symmetric cryptographic function and ensures asymmetric property. TESLA divides time into ‘n’ equal intervals. Each ‘n’ is assigned a corresponding key Kn. The sender appends MAC to the data generated at time interval n, using the secret key Kn. The receiver simply buffers the packets. After some ‘d’ time slot, the sender discloses the corresponding key seed Sn. Using a public one way function F’, the key Kn can be derived from Sn.

To create a key seed chain the sender chooses a terminal seed St and generates St-1 using a one-way function F. Thus, F (S_t) → S_{t-1}, F(S_{t-1}) → S_{t-2}, F(S_{t-2}) → S_{t-3}, F(S_{t-3}) ….→ S_0. For key generation the key seed chain is used in the reverse order (i.e. it starts from S_0). Therefore, F’ (S_0) → K_n. Once the user receives a TESLA seed S_n, he guarantees the authenticity by checking F(S_n) → S_{n-1}. The authenticating key K_n is generated using the one way hash function F’.
In our approach, TESLA is used in creating group membership and node membership certificate, which supports source authentication in the MAODV secure route discovery.

4 SECURE MAODV

The Multicast Ad-hoc On Demand Distance Vector (MAODV) routing protocol [27] constructs a shared multicast tree, which connects the group members. In addition, the MAODV helps the group members to get connected to the multicast tree through the forwarding nodes. Members can join or leave the group at any time. One of the group members is the Group Leader. It initiates a route request at first and initializes the group sequence to one. The Group Leader is responsible for maintaining the multicast sequence number. At regular intervals it generates Group Hello (GH) messages across the network to maintain the multicast sequence number. The multicast sequence number is used to check the freshness of the multicast group.

The Wireless Sensor Network [2] is deployed in a hostile environment. The communication and deployment mode of WSNs makes it insecure. Sensor networks consist of resource constrained devices, implementing a security mechanism. Thus, our proposed authentication framework has the following objectives

- An unauthorized node should not be able to participate in the MAODV routing.
- Non-Group member node should not be able to act as a group member.
- Non-tree node should not be able to impersonate a tree node.

To achieve the above goals, this work proposes an authentication mechanism in which the sensor nodes and base station need to have necessary credentials to participate in the MAODV protocol. All the four types of nodes are used in the implementation. The nodes can be

- A Group Member
- A Group Leader from one among the Group Members.
- A Multicast Tree Member
- A Non-tree Member

The given group certificate and node certificate are the elements of the authentication framework.

4.1 Group Certificate

Every group member has the privilege to initiate a route request to join a multicast tree. It has a Group Membership Certificate, which justifies that it belongs to a particular multicast group. To reduce the communication overhead

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Group Private Key</th>
<th>Life Time</th>
<th>SIGN Group Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Bytes</td>
<td>2 Bytes</td>
<td>2 Byte</td>
<td>2 Byte</td>
</tr>
</tbody>
</table>

Figure 1: Group Membership Certificate

in WSNs, we assume that a node can belong to only one group. The format of the group membership certificate [28] is shown in Fig. 1. It contains the group ID, Group Private Key, Lifetime of the certificate and the Group Public Key used for signing the certificate.

4.2 Node Certificate

All the sensor nodes, whether a group member or non-group member in the network have a certificate called the node certificate. This certificate is issued by a trusted certificate authority (CA). In WSNs, the base station acts as a certification authority. The format of the node certificate is shown in Fig 2. Only nodes possessing node certificates are eligible to participate in routing. The base station pre-distributes the node certificate off line to all the sensor nodes in the network, before deployment. All the nodes know the public key of the Certificate Authority (CA). Thus, there is no need to contact the CA for verification of a node.

<table>
<thead>
<tr>
<th>Node ID</th>
<th>Node Private Key</th>
<th>Life Time</th>
<th>SIGN Node’s Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Bytes</td>
<td>2 Bytes</td>
<td>2 Byte</td>
<td>2 Byte</td>
</tr>
</tbody>
</table>

Figure 2: Node Membership Certificate

4.3 Group Leader

The Group Leader broadcasts the Group Hello (GH) packets to all the valid group members. The previous credentials of the group leader are used to authenticate the GH messages.
4.4 Multicast tree Member
When a non-member joins the Multicast tree, a shared tree is constructed if it is needed. The Group Leader is the root of the Multicast tree. It generates and securely distributes the tree key to the entire Multicast tree members. A node that has the valid tree key will reply the route request.

4.5 Secure Route Discovery
Secure route discovery has two stages. At first, a source node broadcasts the route request and then it receives a route reply. The format of the RREQ Message is given in Fig 3. RREQ has seven fields:

RREQ: (Join Req, Request ID, ID destination group, Group Cert, Source Node Certificate, Start Time, SIGN source private key (……))

The request ID is used to check the freshness of the request. The entire packet is signed using the source private key. A node initiates the Route Request Message [RREQ] in two situations;

Case i - If a group member ‘i’ wants to join a multicast group, then it prepares the RREQ packet and broadcasts it to all its one hop neighbors. If the receiver is a multicast tree node, then it applies validation of the source algorithm and sends a reply to the sender by checking its routing table. The routing table contains the control information of the destination. If the receiver is a non-multicast tree node, then it forwards the request by replacing the outer signature with its own signature and forwards the request to the neighbors. The nodes of the tree maintain a dynamic request table. The format of the request table is shown in Fig 5.

Case ii - if a group member ‘i’ wants to send data to a destination group by creating the multicast tree with valid group members of that session, then it prepares the RREQ and replaces the Join Request field by creating a multicast tree field and the rest of the process is the same as in Fig 7.
RREQ : (Create Tree Request, Request ID, ID destination group, Group Cert, Source Node Certificate, Start Time, SIGN source private key (…))

If a node ‘i’ does not receive a RREP message then it rebroadcasts the request ‘m’ times. Then, the node ‘i’ declares itself as the group leader by sending Group Hello Packets to all the group members.

4.6 Working of Secure Route Discovery

If a node ‘i’ wants to join a multicast tree, the node will broadcast the route request packet to all its one hop neighbors. The non-group member forwarding the RREQ is the forwarding node. The RREQ has two signatures. The signature of the source node certificate is called the inner signature. The entire RREQ packet is signed by the forwarding node and it is called the outer signature.

Algorithm: Validation of the Source Node

// t_r denotes the time when the RREQ is received
// ts denotes the issue time of the RREQ
// D: propagation delay
1. Assume node ‘k’ receives a RREQ at t_r.
2. if ts + D < t_r then
3. Discard the RREQ
4. else
5. if (forwarding node is a trusted node) then
6. Buffer the RREQ packet and store forward node ID in request table.
7. Wait (for group authenticating key to be disclosed.)
8. if (source node ‘i’ has a valid group member certificate) then
9. Send the RREP packet with the following details;
10. Append the tree key and reply node ID
11. Encrypt with the source node public key.
12. else
13. Discard the RREQ
14. end if
15. else
16. Report the unauthorized node to CA.
17. endif
18. endif

If a forwarding node ‘j_1’ gets the RREQ, then its checks the inner signature and stores the sender’s ID as in-hop ID in its request table. The node ‘j_1’ appends its certificate to the RREQ and broadcasts it. Suppose a forwarding node ‘j_2’ gets the RREQ packet from node ‘j_1’; then it checks the outer signature, inner signature and updates the request table. The node ‘j_2’ adds its certificate by replacing the certificate of node ‘j_1’ and broadcasts the RREQ. If a multicast tree member ‘k’ receives the RREQ then it removes the outer and inner signature. The node ‘k’ checks the routing table and sends the RREP packet. The format of the RREP is shown in Fig 4. The working of secure route discovery is given in Fig 7.

i→ * : [ RREQ ]; // node ‘i’ broadcasts RREQ.
  j_1 : [ RREQ ]; // node ‘j_1’ receives the RREQ.
     // it checks inner signature and appends the forwarding Node Certificate.
  j_2 : [ RREQ , Node Certificate of j_1 ];
     // validates & replaces certificate of node j_1.
  j_2→ * : [ RREQ , Node Certificate of j_2 ];
     k : Executes validation of the source node algorithm and sends RREP packet.
  k→ j_2 : [ RREP ]
     j_2 : [ RREP ]; increments the hop count;
     j_1→ j_2 : [ RREP , Node Certificate of j_2 ];
     i : [ RREP , Node Certificate of j_1 ];
     // validates inner signature. Checks the group sequence no. updates multicast tree table, and request table.

Figure 7: RREQ initiated by node ‘i’ and its subsequent actions to establish a secure route.

5 NETWORK PERFORMANCE

The network simulator NS-2 (http://www.isi.edu/nanam/ns/) has been used in evaluating the performance of the secure route discovery. Figure 8 shows the topology of the simulation. Table 1 gives the simulation parameters and Table 2 gives the default MAODV parameters.

The simulated scenario consists of a network with 30 nodes and two multicast groups A and B with 10 members each. All the group members
join the multicast group at the beginning of the simulation leading to the construction of the multicast tree. The field ID is used in identifying the nodes. The sensor with ID zero is the base station, which is responsible for the distribution of certificates. The base station plays the role of the central TESLA certificate authority (CA). Table 2 lists the default values of the MAODV parameters used in the simulation. The node and group certificates in our simulation use a 512 bit public key and 16-byte signature as in [15].

Table 1: Simulation Environment Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Nodes</td>
<td>30</td>
</tr>
<tr>
<td>Pause Time</td>
<td>50 sec</td>
</tr>
<tr>
<td>Simulation Grid Size</td>
<td>500mX500m</td>
</tr>
<tr>
<td>Radio Transmission Range</td>
<td>50 m</td>
</tr>
<tr>
<td>Transmitting power</td>
<td>0.175 mW</td>
</tr>
<tr>
<td>V Receiving power</td>
<td>0.145 mW</td>
</tr>
<tr>
<td>Sensing power</td>
<td>0.00000175 mW</td>
</tr>
<tr>
<td>V Idle power</td>
<td>0.0 mW</td>
</tr>
<tr>
<td>Initial energy</td>
<td>5.0 Joule</td>
</tr>
</tbody>
</table>

Each simulation was run for 100 seconds. After 30 seconds, one group member (node 6) joins the group securely. For each set of experiments, 50 runs were performed. The average values are used in plotting the graphs and these values are compared with the MAODV values [25].

Table 2: Default MAODV Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Allowed Hello Loss</td>
<td>3</td>
</tr>
<tr>
<td>Group Hello Interval</td>
<td>5 secs</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>1 secs</td>
</tr>
<tr>
<td>Lifetime of Route Table Entries</td>
<td>3 secs</td>
</tr>
<tr>
<td>Max. No. of RREQ Retransmissions</td>
<td>3</td>
</tr>
<tr>
<td>Max Time to Wait for a RREP</td>
<td>5 secs</td>
</tr>
</tbody>
</table>

5.1 Performance Metrics

The packet delivery ratio, packet overhead, average delay and average energy in the network are used as the metrics for evaluating the performance.

a) Packet Delivery Ratio (PDR) is defined as the ratio of the total number of data packets received by the multicast group members to the product of the number of data packets sent and the number of group members.

The analysis shows that PDR is 40% high for secure MAODV, because RREQ message collision takes place while broadcasting. The certificate of the sender is appended along with the message. So, the packet size increases.

b) Average delay in the network: In the simulated environment group A is distributed and group B is densely packed. So, the average delay in the network is 15% more for group A when compared to group B. In real time scenario the WSNs are densely packed and hence cause less delay.
c) Energy Analysis: The average energy of the network is calculated as the sum of the energy of the sensor nodes divided by the number of nodes. The simulation shows that the average energy drops to 20% with an increase of 30 numbers of nodes.

The disadvantage is that, it requires clock synchronization and the existence of a private/public key pair between base station and sensor nodes. To authenticate the TESLA key for each node, a one-way hash chain has to be maintained. TESLA keys are distributed to the participating nodes via the offline key distribution center.

6 CONCLUSION

In this work, we have reduced the group membership and node membership certificate. We have introduced a request table, which stores the next hop and previous hop IDs. We have also reduced authentication overhead. All these features are well-suited for low-power devices such as sensor networks.

In this work, we have applied a TESLA-based certificate to secure MAODV for low power Wireless sensor networks. It is proven that we can apply Secure MAODV, which has a negligible impact on MAODV performance during the normal operation of the protocol.

Future Enhancement

The simulation study shows that the TESLA-based Certificate with MAODV is possible with wireless sensor networks. Further, if we create a cluster-based multicast, the performance will greatly improve. The tradeoff between delay and overhead is a critical issue for further study.

REFERENCES

[22] SensorSim: NRL’s Sensor Network Extension to NS-2, Naval Research Laboratory.


