Secure Group Communication in Mobile Wireless Sensor Networks

Nahar Sultana, Eui-Nam Huh*
Internet Computing and Security lab
Kyung Hee University, Korea.
Email: nahar@icns.khu.ac.kr, johnhuh@khu.ac.kr*

Abstract
Mobile sensor networks consist of mobile nodes interconnected by multihop path that has no fixed network infrastructure support. Due to limited bandwidth and resource and also the frequent changes in topologies, sensor network should consider these features for the provision of security. This paper proposes and analyzes a scalable and efficient routing protocol by introducing identity based infrastructure for secure group communication in wireless sensor networks. In a group communication, group merge is one of the operations for multiple member changes in a group. The newly merged group needs a secure route to maintain relationship with other groups. To ensure scalability for proposed ID based routing protocol, the system takes signcryption method which combines signature and encryption which provides a significant cost. Through comparison and analysis we have shown that our protocol has high probability to be resilient for secure communication among mobile nodes.

Keywords: Routing, Group merge, signature and encryption, ID-based infrastructure.

1. Introduction
With the popularization of the internet and evolution of wireless technologies, the use of mobile computing for various kinds of the internet applications has increased significantly in recent years. Sensor network, one of the most popular techniques to support this trend, is a temporal network in which mobile nodes with wireless interface dynamically establish connection without preexisting communication infrastructure. Such networks can be very useful in crucial and vital applications such as the military operations in enemy battlefield, emergencies and rescue operations.

Sensor networks provide economically viable solutions for a wide variety of applications, including surveillance of critical infrastructure, safety monitoring and many health-care applications. As sensor networks are increasingly deployed in such security and safety critical environments, the need for secure communication primitives is self evident. Likewise, the development of secure primitives enables the use of sensor networks in new application. The central goal of this work is to ensure node to node message delivery, even if the sensor network is under active attack. In the presence of attacker, it is an extremely challenging task to maintain correct routing information. Most of proposed routing protocols for sensor networks are optimized for performance in dynamic environment. However, many of these routing protocols have security vulnerabilities from attacks. Moreover, the security of sensor network is more vulnerable than that of wireless networks using fixed infrastructure, so that the security services in the sensor network faces a set of challenges.

The majority of secure routing mechanisms focus exclusively on the prevention approach, since it is the most efficient and effective against known attacks. Many researchers also propose detection and recovery mechanisms.

The rest of this paper is structured as follows. Section 2 describes the related work, Section 3 describes the protocol overview and introduces proposed group merge operation; Section 4 describes the proposed signcryption scheme for routing. Section 5 analyzes the security and performance evaluation of the proposed scheme. Section 6 concludes the paper.

2. Related Work
Due to the broadcast nature of the wireless environment and lack of infrastructure, achieving routing security in mobile wireless sensor network is a complex task [9][10]. Based on the two basic routing
protocols in mobile adhoc networks, DSR (Dynamic Secure Routing) [11] and AODV (Adhoc on Demand Distance Vector) [12] , a number of protocols have been developed to secure the routing in wireless network. SRP [13] assumes the existence of a shared secret between the source and destination to validate the integrity of a discovered route. ARAN [5] uses public key cryptography instead of the shared secret in [14] to verify the discovered route. Both SRP and ARAN ensure only the authenticity but not the privacy of the routing information, intermediate nodes that handle the routing packets can easily find the identity of the communicating nodes. In hostile environments, the privacy of routing information must be protected strictly. Otherwise, the adversaries may deduce important information about the location or mobility of communication parties, therefore locate or attack the targets physically. The anonymity of the routing protocol must be considered as an important part in the secure routing of wireless sensor network.

3. Protocol Overview

In a group communication, for single member changes there are node joining or leaving operation and for multiple member changes group merge is one of the operation. In this type of communication, every group has its own group leader GL. This GL is responsible for keeping relations with other groups. We propose that if two groups merge then the new group can securely communicate with other groups, this time also GL will be responsible. For this secure communication we are going to describe our signcryption scheme to find the secure route. In this section we narrate how the groups can be merged and form a new group.

3.1 Proposed Group merge Operation

Initially every sensor node comprises its own group. A group G first collects information about the current size of each neighboring group. It then proposes to merge with smallest neighbor G' and waits for a response. If that group does not wish to merge with G, then G considers the merge a failure and restarts its merge process by predetermining its smallest neighbor. Favoring the smallest neighbor makes it more likely that groups of similar size will merge. If G' also proposes to merge with G, the two groups merge to form a new group \( \gamma \). Consider a group G at an intermediate stage of the grouping process. Some portions of the nodes in group G have neighboring nodes not in the group. We refer to these nodes as edge nodes a1, a2, b1, b2 as figure 1. If all of a node’s neighbors belong to its group, then we refer to it as an interior node. The edge nodes are responsible for communicating with neighboring groups and forwarding the results of merge agreements to the interior nodes like figure 1. Since different edge nodes will hear from different neighboring groups, they must communicate with each other to decide on a merge target (i.e. the group to which to send a merge proposal). To initiate a merge, each merge node floods its group with the size and ID of each neighboring group it borders.

![Fig 1: Merging groups](image)

Exchanging Merge Proposals:

Once the edge nodes know about all of the neighboring groups, they each independently compute the neighboring group G' with the smallest size and any edge node that borders G' will broadcast a merge proposal to that group. If the merge target refuses to merge (by announcing that it has already selected another group) then the edge nodes propagate the refusal to the rest of the group and the edge nodes once again compute the smallest neighboring group. If G' also selects G as a merge target, then the two groups will merge.

Merging:

If groups G and G' agree to merge, they will form a new group \( \gamma \). As a result of this merge, all of the nodes in \( \gamma \) must compute the new group ID \( ID_\gamma \) .record information about the group they merged with. First all nodes in the group can independently compute the new group ID as,

\[
ID_\gamma = \begin{cases} 
  h \left( ID_G, |G|, ID_G, |G| \right) & \text{if } ID_G < ID_G \\
  h \left( ID_G, |G|, ID_G, |G| \right) & \text{if } ID_G > ID_G 
\end{cases}
\]
The new group ID incorporates the IDs and sizes of both of the old group. The method for computing the new group ID is designed to avoid collisions in the group ID space. Each node in group G also updates its merge table such that \( M[i]=(G \mid G') \). This information will be used later to authenticate the merge process.

4. Introducing the signcryption scheme

We apply the signcryption scheme to our secure routing protocol for adding the efficient security features. The first requirement in any signcryption scheme is to agree on a common key between the sender and receiver. Signcryption is a scheme which combines a function of digital signature scheme with a symmetric encryption algorithm. A digital signature scheme is used for the authentication of messages and an encryption scheme is used for the confidentiality of messages. Signcryption offers these two properties at the same time and a more efficient computational cost than the traditional signature then encryption method.

4.1 Proposed Protocol

In this section, we introduce our proposed secure routing protocol in group communication for wireless mobile sensor networks. Our goal of this paper is to design a secure communication in a group by introducing secure routing protocol to make communicating new merged group anonymous to the intermediate groups in the routing path, thereby protecting the privacy of communication groups and routes. Our proposed protocol can be divided in the following ways:

\( i \) In a group communication for multiple member changes we apply group merge. After merging two or three groups, they formed into a new group.

\( ii \) For secure communication of that new group with the existing groups needs a secure route.

\( iii \) For the secure route we can divide it into secure route request phase and secure route response phase.

\( iv \) To find out the secure route we apply signcryption scheme for adding better security.

In our scheme we assume the newly formed merged group has its own group leader as well. All group leaders are works as sender/receiver node and also intermediate nodes. In a group every sensor node is keeping updated by its group leader. In which possible ways the groups can be merged, we have already discussed in section 3.1. Now we discuss the route request phase and route reply phase.

\( v \) The initial assumption is there will be two multiplicative groups \( G_1 \) and \( G_2 \) and the weil pairing \( e \) defined as \( e:G_1 \times G_1 \rightarrow G_2 \). In addition to these, hash functions \( H':\{0,1\} \rightarrow Z^*q \), \( H:Z^*q \rightarrow \{0,1\} \) and \( H_1:G_2 \rightarrow \{0,1\} \).

Algorithm for secure route:

\( <\text{sending RREQ packet}> \)
Sender node calculates security parameter and then signs this message before sending a packet;
\( <\text{receive RREQ packet}> \)
Receiver node compares security parameters and checks the signature;
if the receiver node is the destination then it prepares to send RREP packet;
else (the node makes any necessary modification)
the node forwards packet to the next

**Step 1: Route Request Phase**

For any node \( S \) in the network, it can have the routing path information from \( S \) to the destination \( D \) to perform the following procedure. We assume the intermediate nodes in the routing path 1-k. The form of route request packet,

\( <\text{RReq, SID, DID, seq(S, D), Sig (M), intermediate ID list}> \)
\( (M= (RReq\mid SID\mid DID\mid seq)) \)

A node \( S \) that initiates the route discovery protocol perform the following procedure,

\( i \) When \( S \) wish to send message to find the route it obtains its public key and private key pair \((P_{u_S}, P_{r_S})\) from the key generation centre by sending its identity. Similarly, the destination node \( D \) also can obtain its key pair \((P_{u_D}, P_{r_D})\).
ii) Generate a random string $a \in \mathbb{Z}_q^*$ and computes the following,

a) $R = a \cdot Pr_S$
   $R' = (R \| H(e(Pu_D, Pr_S) \| M)$

b) $S = a \cdot H(R')$, $Pu_S$
   $= a \cdot H'(R \| H1(e(Pu_D, Pr_S) \| M) \cdot Pu_S$

c) $K_s = H''(e(Pu_D, Pr_S) \cdot H(R'))$

d) $C = K_s \oplus M$

iii) Using the values generated in (ii) make the following packet and broadcast it,

\[<RREQ, SID, DID, seq, Sig(M), intermediateID, list, R, S, C>\]

iv) The source sends routing request message authentication information $T = (r, V)$ and created the values which are signed. Here $r, V$ are the security parameter.

v) The intermediate node $i(1 \leq i \leq k)$ that receives route request packet and does the following,

a) Once an intermediate node $i$ receives a route request packet (RREQ), it first checks its routing table.

b) If the sequence number $seq$ has already been recorded in the routing table, node $i$ simply discard this RREQ packet. If the seq is not in the routing table node $i$ considered as intended destination node.

c) If node $i$ unsigncrypts the message using $K_D$(which is derived from its private key $Pr_D$), it means node $i$ is the intended destination node of the route request packet and the route request phase is ended. At that time,

\[K_D = H''(e(Pr_D, S))\]

\[M = K_D \oplus C\]

Consistency,

\[K_D = H'(e(Pr_D, S)) = H''(e(Pu_D, a \cdot H(R'), Pu_S) = H''(e(Pu_D, Pr_S H(R'))) = K_s\]

Otherwise, the whole process is going on as before.

d) To verify the message $M$ has reached properly, the destination node $D$ computes $H'(R || H(e(Pu_D, Pr_S) || M)$ and accepts the signature only if $e(Pu_D, S) = e(Pu_D, R H(R'))$, rejects otherwise. This verifies any message tampering on route since,

\[e(Pu_D, R H(R) H1(e(Pu_D, Pr_S) || M) = e(Pu_D, a \cdot Pr_S)\]

\[= e((Pu_D, Pr_S) H(R H1(e(Pu_D, Pr_S) || M)) = e(Pu_D, a \cdot H(R || H1(e(Pu_D, Pr_S) || M)) \cdot Pu_S\]

If the message were tampered on route, then this verification would detect the change. The signcryption is valid one if both are equal and it is rejected if they are not equal since it implies that the message has not reached to the intended destination. When the destination node receives the message it checks the destination address and also checks $T$ for authentication. If the authentication is successful then the destination node is ready to reply a message. Otherwise the packet is dropped.

**Step 2: Route Response Phase**

The destination node generates an RREP packet and sends the source node. The destination node unicasts an RREP packet with a message for authentication back along the reverse path to the source node. The RREP packet contains the following $<RREP, SID, DID, seq(D), Sig(M)>$. Also the node adds $T$ because the source node can trust the right reply to message. The computation method of $T$ in route response follows the similar way in RReq.

5. Security Analysis and Performance Evaluation

5.1 Security Analysis

We can show that our scheme can provide confidentiality, authentication, forward secrecy and non-repudiation.

a) Confidentiality is achieved by encryption.

b) Authenticity is guaranteed by having the signature since the sender uses its private key to signcrypt.

c) To check whether the scheme is forward secure, suppose that the long term private key of $S$, $Pr_S$ is compromised. Now if an adversary knows the values($R, S, C$) of an earlier session along with $Pr_S$ and tries to get back the message it has to compute

\[K_s = H''(e(Pu_D, Pr_S) \cdot H(R H1(e(Pu_D, Pr_S) || M)\]

But “M” and “a” are not known to adversary to compute this key. Also $H(R H1(e(Pu_D, Pr_S) || M)$ cannot be computed from the given ($R, S, C$) and $Pr_S$.

Thus, it is proved that our scheme is forward secure.

5.2 Performance Evaluation

In the following steps, we analyze the computational cost and the communication overhead of the proposed protocol. For our scheme the communication overhead for our protocol is as follows,

\[CO = \sum_{i=1}^{x} (n |Hl + nl El + nl Sl + n \cdot (packet*)8)\]
Where, CO stands for communication overhead, $n_i$ is the number of execution of $i$th node, |E| is the encryption, |S| is signature, |H| stands for hash function and packet is RREQ, RREP. Total overhead is value of communication overhead and computation cost

$$TO=\sum_{i=1}^{X} \text{(CO * computation cost)}$$

Where, TO is the total overhead.

**Table1: Comparison of proposed protocol with others**

<table>
<thead>
<tr>
<th>Scheme</th>
<th>ARAN</th>
<th>SRP</th>
<th>Proposed protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key distribution</td>
<td>Public key(RSA)</td>
<td>Public key(ECC)</td>
<td>Public key (ID-based Signcryption)</td>
</tr>
<tr>
<td>Intermediate node authentication</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Communication overhead</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Computation cost</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Cost in computation and communication</td>
<td>Cost(signature)+Cost(Encryption)</td>
<td>Cost(Encryption)+cost(Hash)</td>
<td>Cost(signature)</td>
</tr>
<tr>
<td>Key management</td>
<td>Centralized</td>
<td>Centralized</td>
<td>Distributed</td>
</tr>
</tbody>
</table>

Fig. 2 shows that the overhead of the proposed protocol in terms of routing load is very low because computation cost of signcryption is very low.

**6. Conclusion**

In this paper, we have focused on efficient group communication by changing multiple members. For secure communication of new group with the existing groups we have proposed an ID based signcryption routing scheme. This protocol has an advantage that it does not need to authenticate the public key because it uses the ID based scheme. It can reduce network resources and communication overheads than the conventional secure routing because of the features of identity based signcryption. We have also shown the simulation result to prove the efficiency of our scheme.

**References**


