Secure and Robust Key Management Scheme for Ad-Hoc Sensor Networks

A.S. Nagesh

Department of Electrical and Computer Engineering, College of Engineering

1. Introduction

Ad hoc networks are infrastructure-less wireless networks, which are formed on the fly. There are different types of ad hoc networks of which sensor network is one of them. A typical sensor network consists of thousands of highly resource constrained sensor nodes. The self-organizing nature of these networks makes them very effective in security sensitive applications such as health, target surveillance, military, disaster recovery programs and personal area networks amongst the others. Similar to traditional networks, these networks are also pruned to various kinds of security threats. Security infrastructure for these networks should to be built in such a way that it provides low complexity, simplicity of implementation and allow the nodes to undergo a secure communication without having to frequently access a central trusted authority.

In the proposed scheme, key pre-distribution technique is followed, where in a trusted authority, prior to the deployment phase distributes certain number of key shares to every node in the network. The resiliency of the network to node captures is increased by storing only partial key shares of other nodes in each node's key ring. This means that to compromise any one full key, it is required to compromise q distinct shares of that particular key. The message is passed over the communication links securely by encrypting it with a series of partial shares of the symmetric decryption key held by the destination node. One simple way to implement this is to use XOR operation. Suppose a full key is obtained from the XOR operation of several partial keys then the message encrypted with the all those partial keys will be equivalent to message encrypted with the full key. This is one type of logic that can be applied for dividing a key in to partial shares.

2. Related work

In general, according to [1], key management schemes are broadly classified in to four different categories based on the type of cryptography employed in securing the keys required for communication and whether they rely on centralized or decentralized method to distribute the keys securely over the network.

Centralized asymmetric approach is a very direct solution for key management in networks, where in a central certificate authority is employed to issue a certificate by signing the public key of the individual nodes. This type of key management service is usually employed in traditional wired or wireless networks. To avoid the problem of single point of failure, Zhou and Hass [2] proposed a decentralized asymmetric method, where in the CA's service is distributed to a set of specialized nodes as in partially distributed scheme or to all the nodes in the network as in fully distributed scheme. These schemes are based on (k, n) threshold cryptography where the power to recreate the CA's private key is distributed among n nodes. Since the schemes use asymmetric cryptography, it is not feasible to use them on resource constraint sensor nodes. In sensor networks, based on hierarchical architecture, some of the deployed nodes are usually made slightly powerful and capable to control and monitor other sensor nodes in the network. These high-energy sensor nodes are called cluster heads (CH). Many security protocols [3] proposed in recent years use symmetric cryptography in centralized fashion. Recently Eschenauer and Gligor [4] have proposed a random pre-distribution scheme for Distributed Sensor Networks based on probabilistic key sharing. Each node is pre-initialized with a random subset of m keys $(O(m) << O(n^2))$. Based on the key pre-distribution technique Chan [5] proposed three new mechanisms namely q-composite scheme, multi-path key reinforcement scheme and random pair-wise key pre-distribution scheme. In these schemes the keys stored in the nodes are the actual secret keys that are used to secure communications between them.

3. Proposed Key Management scheme

The proposed key management scheme is based on key pre-distribution technique. Let S specify a set of keys (K_1, K_2, K_3..... K_N) present in a large key pool of size N. Further each key in the key pool is again divided into multiple shares such as K_{11}, K_{12}, K_{13}.....K_{21}, K_{22}, K_{23}..... K_{31}, K_{32}, K_{33}..... and so on. In general the entire key set U can be written as K_{ij} where $i = 1$ to n and $j = 1$ to q. The assignment of keys is done in a predefined fashion by a trusted authority. Each node is given one

distinct full symmetric key called the decryption key from the sets S that is used to decrypt the incoming messages and some partial shares of other nodes' decryption keys. Each key in the set S and U is assigned a key identifier prior to the deployment phase. The keys are stored in every node's key ring along with their key identifiers. When two nodes are required to undergo secure communication, the source node will obtain representation of the destination node's decryption key with the help of key identifiers. The source node can check in its key ring to determine whether it holds a partial key for the destination node. If so, the source node encrypts the message and sends it through a set of intermediate nodes. The message is encrypted in each intermediate node using the partial keys stored in them for the destination node. After the message has passed through all intermediate nodes, the final encrypted message will be equivalent to the message encrypted with the destination node's symmetric decryption key. Finally when the message reaches the destination node, it is decrypted using the destination node's full decryption key.

4. Analysis

Let us consider that each of the decryption keys is divided into q shares. For each node to be able to reach all other nodes in the network, q is the minimum number of shares required to be stored in every node's key ring. To increase the network reach ability in case of node failures or due to nodes falling out of transmission range, each node is also given r redundant shares. However, the shares stored in every node is distinct i.e. no node stores more than one share of the same key. The value of r varies according to the number of nodes in the network. If the network is large, the value of r should be chosen in such a way that it suffices the required network reach ability.

Distribution of key shares: Let each key in the key pool S be divided into q shares and if there are n number of nodes in the network, the total number of shares obtained is $q \times n$. The share distribution is done in such a way that the nodes will not get any shares of their own decryption key. Each node in the network is given q distinct shares from the other nodes' decryption key. This is given by:

$$({}^{(n-1)q}C_q)\ ({}^{(n-2)q}C_q)\ ({}^{(n-3)q}C_q)\ \ldots\ldots\ldots\ldots\ldots\ldots\ ({}^{q}C_q)$$

First term gives the number of ways q distinct key shares can be selected for any one node from the remaining $n-1$ nodes' decryption keys. Second term represents the number of ways q distinct key shares can be selected for the next node from the remaining $n-1$ nodes leaving the q distinct shares that have already been selected. Similarly, the successive terms represents the numbers of ways the key allocation is done for the remaining nodes in the network.

To give r redundant shares: The r redundant shares are given to each node from the other nodes' decryption keys such that a node will not get the same key shares that has in its key ring. If m is the number of key shares stored in a node's key ring and q is number of distinct key shares it holds then the number of redundant shares $r = m - q$. The number of ways to give r redundant shares is:

$$({}^{(n-1)q-q}C_{(m-q)})^n$$

5. Observations

If the shares in all the nodes are distinct then the attacker has to capture at least q nodes to capture some x full keys, where x varies from zero to maximum of q. With the redundant shares the attacker's probability of compromise increases because he/she can compromise some full keys by compromising nodes less than q depending on the value of r (redundant shares). On the other hand giving redundant shares will increase the network reach ability. Hence the value of r should be chosen such that it provides a good trade off between network reach ability and security.

6. References

[1] Arno Wacker, Timo Heiber, Holger"*Key-Distribution Scheme for Wireless Home Automation Networks",* IEEE CCNC'04.
[2] L. Zhou and Z.J. Hass, "*Securing Ad hoc networks",* IEEE Network Magazine, vol 13, no.6, November 1998
[3]"*LiSP, Light Weight Security Protocol for Wireless Sensor networks"*
[4]L. Eschenauer and V. D. Gligor *"A key-management scheme for distributed sensor networks"* November 2002.
[5] H. Chan, A.Perrig, D.Song,"*Random Key Predistribution Schemes for Sensor Networks",* IEEE Symposium on Security, May 2003.