DYCRASEN: A Dynamic Cryptographic Asymmetric Key Management for Sensor Network using Hash Function

D.Saravanan
Assistant Professor
Pavendar Bharathidasan college of Engineering & Technology,
Tiruchirappalli 620024,
Tamilnadu

D.Rajalakshmi
Senior Lecturer
Shri Angalamman College of Engineering & Technology,
Tiruchirappalli 621105,
Tamilnadu

D.Maheswari
Lecturer
Pavendar Bharathidasan college of Engineering & Technology,
Tiruchirappalli 620024,
Tamilnadu

ABSTRACT

In sensor networks security is an important issue. Mission critical networks show great potential in emergency response and recovery. It is challenging to design a key management scheme to fulfill the required attributes for secure communication. The Secure Group Communication (SGC) requires common network wide key for confidentiality of control messages and data reports. The group key should be updated when a node enters inoperative state. Each member of a group of users can compute a common key for secure communication. We define Asymmetric key pre-distribution scheme in terms of storage. The complex encryption and decryption operations are replaced by hash functions and simple AND operations. This proposed scheme minimize the storage computation and computation cost.

Keywords

Key Management, Sensor Network, Hash Function, Asymmetric Key.

1. INTRODUCTION

Sensor networks are used in many applications like military sensing and tracking, environment monitoring, patient monitoring and tracking. Sensor network usually consist of a large set of distributed low power sensors scattered over the area to be monitored. Sensors have the ability to gather data, process and forward it to a central node for further processing. The energy constrained nature of the sensor networks and deployment of sensor nodes in a hostile environment makes the problem of providing security to sensor networks challenging. In a sensor network operating in a battle field, we should encrypt each message from central node (sink node) and every data reports from sensor nodes to central node and messages exchanged among sensor nodes to protect the message from possible enemy eavesdroppers. This type of application demands Secure Group Communication (SGC) model in sensor networks. Security of messages in such SGC model can be achieved by using common group key shared by the group of sensor nodes. One of the important feature of SGC in sensor networks is handling group dynamics (ie., new nodes may enter the area at any time and some of the existing nodes may move out of the area or a node may be compromised by adversaries).

Key distribution is a open problem in cryptography [1]. A group of users of a public network would like to use encryption and authentication algorithms to communicate securely to apply this scheme they need a common key with which to encrypt and decrypt messages they will send to each other. The problem is how to design an efficient protocol by means of which the members of the group can establish a common key. A frequently used approach is KDC (Key Distribution Center). The scheme implemented by the KDC to give a key for each set of users is referred as key distribution scheme (KDS). In this paper we propose a Asymmetric key management scheme. A sensor network is generally designed for deployment in open unmonitored environments. Due to large number of sensor nodes lack of information about deployment hardware capabilities of sensor node, key management is complex with advances in cost effective sensing, computing and communication wireless devices, current machine critical systems are composed of mobile autonomous and wireless devices. Examples can be formed in health care systems, automatic networks, emergency rescue and disaster recovery and so on. It is important to support secure communication with the following attributes: Data integrity, Data confidentiality and Authentication. To provide secure communication system cryptographic key should be employed. In order to achieve forward access control the group key should be changed when a node becomes inoperative if common group key is used. Re keying is a process of updating a group key which is required to ensure that current sensor nodes in the group can communicate securely. The different types of key management techniques are a trusted server scheme for key management between nodes [2], which is not suitable for sensor networks.

2. RELATED WORK

For secure communication sensor networks use symmetric key techniques [3]. The main advantage of symmetric key techniques is its computational and energy efficiency. Secret keys are distributed among nodes before they are deployment.

The challenge for the key distribution scheme is to use small memory size to establish secure communication among a large number of nodes and achieve good resilience. The goal is to prevent adversaries to use the network. Due to lack of support for authentication and confidentiality [4] is not suitable for mission critical applications. To support data integrity, authentication, confidentiality, we consider Asymmetric key for secure communication.

Public – key based approaches were originally proposed to provide solutions to secure communications for the internet, where security services rely on a centralized server, and security service for mission-critical applications may suffer from low availability and poor scalability due to the low reliability and poor connectivity of networks. To improve resilience to break-ins in networks, Zhou and Hass tailor the certificate-based approaches to networks and present a distributed public key management scheme for sensor networks, where multiple distributed certificate authorities are used. To sign a certificate, each authority generates a partial signature for the certificate and submits the partial signature to a coordinator that calculates the signature from the partial signatures. Kong et al. describe a similar but fully distributed scheme [5], where every node carries a share of the private key. However such a system does not provide the verifiability property and hence, is vulnerable to the Sybil attack, where an attacker can claim multiple identities, and cheats honest nodes with the fake partial certificate. To improve security service availability and system scalability, [6] propose a self-organized public key management system, where user issues certificates based on their personal acquaintances. Each user maintains a local certificate repository. When two users want to verify the public keys of each other, they merge their local certificate repositories and try to find (with in the merged repository) appropriate certificate chains that make the verification possible. However, it yields low security assurance when Sybil attacks are present due to the lack of trust anchor, since Sybil attackers can easily defeat reputation and threshold protocols. Zhu et al. present two efficient and robust key management schemes for large scale networks to resist active attacks. The certificate-based schemes presented in [7] are designed for dynamic networks and can adapt to changing topology of networks with efficient memory usage. But they require the help from neighboring nodes for authentication. In this case, if the number of illegitimate nodes is larger than a threshold, they may generate valid certificates through the collusion. For high security assurance and low communication overhead a self contained public key is approached. Identity based cryptography [8] allows to derive an entity's public key from its identity by reducing the need for public key certificates. The fine grained key updates may introduce large communication overheads.

3. OBJECTIVE

To guarantee a secure communication we need to have public-private key pairs to seek efficiency in storage and computation a small number of key pairs and distribute a small number of key copies to each node. The key management to be desired should be memory efficient for key storage and computationally efficient during encryption and decryption. To simplify security each node wants to use a small number of public key to encrypt the outgoing messages and small number of private keys to decrypt the incoming messages.

4. MOTIVATION

The number of levels in the binary tree will be more when the group is large, which increases the number of keys to be stored by each sensor node. Extending this to M-ary reduces the height of the tree by reducing the number of keys at each node. In [9], two keys are maintained at every level of tree, extending the scheme to M-ary m keys will be maintained.

5. PROPERTIES OF M-ARY TREE

Each interior node has at most 'm' children and each path from the node to a leaf has the same length.

6. ASYMMETRIC KEY DISTRIBUTION SCHEME USING HASH FUNCTION

Distribution phase and key computation phase are the phases of Asymmetric key pre-distribution scheme. During the distribution phase the trusted authority first gives secret key to users, then distributes public keying material to the keying material server. During the key computation phase each privilege subset P Є P, using the secret keys received in the distribution phase and pieces of public keying material retrieved from the keying material server is able to compute this common session key associated with P.

7. MODELS AND NOTATIONS

The sensor network composed of 'n' sensor nodes which are organized as m- ary balanced tree with sensor nodes at the leaf. The tree is maintained by central node. The group key is used to encrypt the data traffic. Every sensor node shares a private key with central node which is used to communicate with the central node. The auxiliary key is used to encrypt the new group key. Each node has the capability to compute a one way hash function H as in [10,11] & is capable to update auxiliary keys after getting new group key using the function F(Auxiliary key, new group key← (Auxiliary key),AND(new group key)

8. ENCRYPTION AND HASHING

By replacing encryption with Hash function the method used to communicate the new secret key is as follows: central node computes hash (as in [10, 11]) of a shared key (key known to central node and authorized node) say k_s i.e.,$H(k_s)$ of the encryption key and AND's with new secret key k^{new} to be communicated($k^{comm} \leftarrow H(k_s)+k^{new}$). Upon receiving k^{comm} nodes having k_s compute $H(k_s)$ and AND's with k^{comm}. Which yields new secret key k^{new} ($k^{new} \leftarrow H(k_s)+k^{comm}$).

9. HASH BASED KEY DISTRIBUTION METHOD

The encryption keys computed using [12] are used to communicate new group key to the existing nodes without encryption. In the figure S5 & S6 are the compromised nodes the encryption key computed using the protocol [12] are KEK={$K_{10,}$ $K_{12,}$ $K_{13,}$ $K_{0,}$ K_3}. New group key GK' is distributed to the remaining nodes using hash method to communicate new group key for the nodes S0,..S3 central node computes the hash key K_{10} ($H(K_{10})$) and this with new group key. Which yields $K^{S0,..S3} \leftarrow (H(K_{10}))$ AND GK'.

Similarly the messages send to existing group members from central node are $K^{S8,..S11} \leftarrow (H(K_{12}))$ AND GK', $K^{S12,..S15} \leftarrow (H(K_{13}))$ AND GK', $K^{S4} \leftarrow (H(K_0))$ AND GK'and $K^{S7} \leftarrow (H(K_3))$ AND GK'. The nodes will compute the new group key GK' by ANDing received message with the hash key known to them. The operations performed to avoid decrypting the messages from attackers are 1.

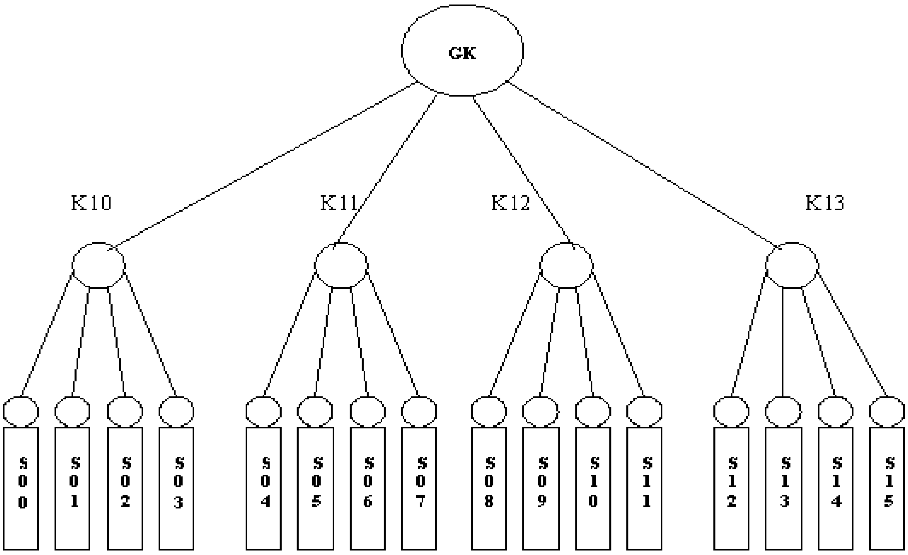

Figure 1: Group key distribution using m-ary tree techniques

The node remaining along the path from the leaving point will compute new auxiliary key 2. The key used to compute the hash value is incremented by one to communicate new group key securely encryption is used along with hash value and AND operations. Hence, communication overhead is reduced.

10. CONCLUSION

In this paper we presented A Dynamic Cryptographic Asymmetric key management scheme for sensor networks using Hash function. Sensor nodes move from one monitoring area to another frequently, and deployment of sensor nodes in a hostile environment allows node compromise. To achieve confidentiality group key is required and the key should be updated when a node is compromised. The tree based key management proposed in this paper computes new group key and distributes it to the current group members efficiently in terms of storage, communication and computation. The storage of central node is reduced from O($\log_m$N) from O($\log_m$N/2). The New group key is distributed to the existing nodes using hash function and AND operations.

11. REFERENCES

[1] C.Blundo and P.D'Arco, "The key establishment problem,"in foundations of security analysis and design FOSAD 2001-02, LNCS 2946. Springer-Verlag, 2004, pp.44-90.

[2] B.C.Neuman and T.Tso,"Kerberos: An Authentication service for computer networks", IEEE communications, vol.32, no.9, pp.33-38, September 1994.

[3] S.A.Camtepe and B.Yener," Combinatorial design of key distribution mechanisms for wireless sensor networks," in Proc.9th Eur.Symp.Research in computer security,2004,pp.346-358.

[4] H.Chan, A.Perrig, and D.Song,"Random key pre distribution schemes for sensor networks," in Proc.IEEE Symp.Research security privacy,2003,pp.197-213.

[5] J.Kong, P.Zerfos,H.Luo,S.Lu and L.Zhang,"Providing robust and ubiquitous security support for mobile ad-hoc networks,"in proc. 9th IEEE Int.Conf.Network Protocols,2001,pp.251-260.

[6] S.Capkun, L.Buttyan, and J.P.Hubaux," Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile comput., vol.2,no.1,pp.52-64, Jan/Mar. 2003

[7] B.Zhu, F.Bao, R.H.Deng, M.S.Kankanhalli, and G.Wang, "Efficient and robust key management for large mobile ad-hoc networks," Comput.Netw.J.,vol.48,no.4,pp.657-682,Jul.2005.

[8] D.Boneh and M.Franklin,"Identity based encryption from the weil pairing," SIAM J.Comput., vol.32,no.3,pp.586-615,2003

[9] I.Chang, R.Engel, D.Kandlur, D. Pendarakis and D.Daha. "Key management for secure internet multicast using Boolean function minimization technique". ACM SIGCOMM'99, March 1999.

[10] N.F.P.180-1. Secure hash standard. Draft,NIST, May 1994.

[11] R.Rivest. The MD5 message-digest algorithm.RFC 1321,April 1992.

[12] A.S.Poornima, R.Aparna and B.B.Amberker, "storage and Rekeying cost for cumulative member removal in secure group communication", International journal of computer science and network security, Vol.7 No.9 pp.212-218,2007.