International Journal of Advanced Research in

Computer Networking,Wireless and Mobile Communications

Volume: 1 Issue: 2 08-Mar-2013,ISSN_NO: 2320-7248

Location Based Key Management for Wireless Mission-Critical Networks

Manjula.R(11msc0092) and Bhavya.S (11msc0081) School of Computing Science and Engineering VIT University , Vellore - 632014 , TamilNadu, India

Abstract :

In this paper, we study about location based key management scheme in wireless mission-critical networks. A challenge of the key distribution scheme is to use small memory size to establish secure communication among a large number of nodes and achieve good resilience. In this paper, we present a new paradigm of public key management scheme based on combinatorial design where nodes combine more than one key to encrypt and decrypt every message. Here key allocation scheme guarantees that a set of keys held by one user is not a subset of keys held by any other user. It is challenging to design a self-constrained key management scheme in current wireless ad hoc networks. In this system we propose to support secure communications with the attributes of data integrity, authentication, confidentiality, non repudiation. To build a secure communication system, usually the first attempt is to employ cryptographic keys.

1. Objective

The Aim of this paper is to provide secure communications, such as data integrity, authentication, confidentiality, non-repudiation, and service availability in the Mission-Critical Wireless Ad-Hoc Networks.

2. Introduction:

With the advances in cost-effective sensing, computing, and communication wireless devices, current mission-critical systems are composed of mobile, autonomous, wireless devices. We can find these in automotive networks, health care systems, critical infrastructure monitoring, military applications. There are emerging needs of secure communications in mission-critical applications over wireless ad hoc networks like emergency it is important to support secure communications in “anywhere”, “anytime” and “anyhow” manner with following attributes: data integrity and service availability. Public-Key Cryptography schemes have advantages over the symmetric systems.[1]However, characteristics of mission-critical ad hoc networks pose the following new challenges for the design of public key management schemes that would support secure communication over wireless ad hoc networks: (1) Unreliable communications and limited bandwidth: Network may be partitioned due to the shared nature of wireless links. Moreover, a network may be partitioned frequently due to node mobility and poor channel condition. Certificate exchange for communication cannot be ignored. (2) Network Dynamics: Mobility increases complexity due to nodes leaving and joining the ad-hoc network frequently. (3)Large Scale: The number of ad hoc wireless devices deployed at an incident depends on specific nature of the incident. An ad-hoc network should be capable of boarding more mobile devices if essential. Therefore, newly deployed devices and previously deployed devices should necessarily trust each other. (4)Resource Constraints: The wireless devices usually have limited bandwidth, memory and processing power. Among the given constraints, communication bandwidth consumption and memory are two big concerns for key management .Wireless bandwidth is the

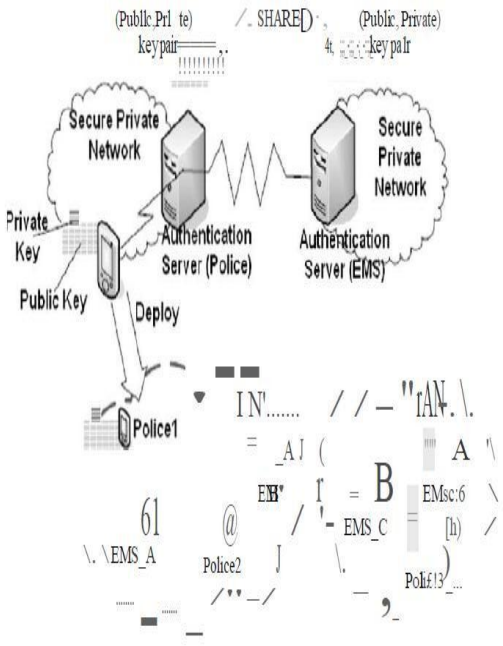
insufficient resources in wireless network. As the requirement on network size is increasing, memory concern for key storage is more and more evident. (5) Vulnerability to the Sybil Attack: Wireless communications are prone to both active and passive attacks. The Sybil attack is an active attack and particularly detrimental to mobile ad hoc networks. When the Sybil attack happens, an attacker can claim multiple identities and the fake identities can easily defeat reputation, where a legitimate node must rely on majority of nodes to reach decisions. Therefore, a node should not trust others unless the node can infer someone else is trustable from local information. Given the above challenges (1) and (2), a node in a network may encounter untrustworthy peers and unreliable communication. Therefore, we need a self-contained key management scheme. Before mobile devices are dispatched to that area, they are able to communicate securely with the trusted authentication server in their domain center, and get prepared before their deployment. Once the wireless devices are dispatched into the incident area, the centralized trusted server loses control of these devices and the mobile devices cannot trust anybody if local information cannot authenticate it. In this paper, we design a self-contained public-key management , where all necessary cryptographic keys are stored at individual nodes before nodes are deployed in the incident area. The required storage space for traditional self-contained public key management schemes is of O(n) order. With challenges (3) and (4), storage space at individual nodes may be too small to accommodate self contained security service, when network size n is large. Hence, we present a Cryptographic Key management , which scales logarithmically with network size, O(log n), with respect to storage space.[1]

3. Implementation:

We have implemented a key-management scheme under the context of the trustworthy cyber infrastructure for the power grid (TCIP), with C. In our implementation, nodes get their subset of private keys, unique IDs and all public

keys via the SSL channel from a trusted authority before secure communication. When a node need to send a message to another node (the receiver), This is sends a plain-text message (along with its ID). The receiver then encrypts its ID with the sender's public keys, and sends the encrypted message to the sender. The sender can encrypt the message by using the receiver's public keys. And the receiver can then decrypt the message using its privacy keys. We measured the encryption and decryption process time that was taken to encrypt and decrypt a message. In location based key management scheme uses small set of cryptographic keys, a sender uses multiple keys to encrypt a message and a receiver needs multiple keys to decrypt the message. We then use the public key cryptography as follows: Each node possesses a unique combination of private keys, and knows all public keys. The private key combination pattern is unambiguously associated with the node ID. Means, if a sender A wants to send a message to receiver B, A will first acquire B's ID to infer a set of private keys owned by B. Then A will encrypt the message with the public key set that corresponds to the private keys owned by B. We have evaluated this with respect to the communication overhead for key management, memory footprint. However, before the system detects break-ins, a majority of network nodes under this will operate securely even when a small amount of nodes are compromised.

Fig.1. The below figure demonstrates two agencies (police department and emergency medical service (EMS)) maintaining the same private and public key pool through an secure connection. Before deployment, agencies pre-distribute keys to devices. After devices are dispatched into the incident areas, it is high and unsafe to communicate with agencies. So all the devices authenticate messages according to the pre- distributed keys.[1]



4. Existing System:

In secure communication, wireless sensor networks use symmetric key techniques. In symmetric key techniques, secure keys are pre-distributed among nodes before their deployment. A challenge of the key distribution scheme is to use small memory size to establish secure communication among a large number of nodes and achieve good resilience. Public-key (certificate)-based acts were originally proposed to provide solutions to secure communications for the Internet, where secure services rely on a centralized certification server. The certificate-based approaches to ad-hoc networks and present a distributed public-key-management scheme for ad-hoc networks, where multiple distributed certificate authorities are used. To sign a certificate, each authority generates a partial signature for the certificate submits the partial signature to a coordinator that calculates the signature from the partial signatures. 4.1 Disadvantage: 1. Lack of support for authentication and confidentiality. 2. single-point failure of the centralized server is able to paralyze the all network, which makes the network extremely vulnerable to compromises and denial-of-service attacks. 3. Total number of keys held by each user is O (n) traditional key-management 5. Proposed System:

In this system we propose to support secure communications with the attributes of service availability. Let us assume a group of people in that area, who wants to exchange correspondence securely among each other in a pair-wise fashion .The key pool of such a group, consists of a set of private–public key pairs, and is maintained by an offline trusted server. Each key pair consists of two mathematically related keys. The Ith key pair in the key pool is represented by (priv ^i, pub^i). To support secure communication in the group, every member is loaded with all public keys of the group and assigned a distinct subset of private keys. Every person keeps a predetermined subset of private keys, and no one else has all of the private keys in that subset. For a public–private key pair, multiple copies of the private key can be held by different users. A message is encrypted by multiple public keys, and it can only be read by a user who has the corresponding private keys. 5.1 Advantage: 1. To Support secure communications among the users in Mission-Critical Wireless Networks. 2.

In this key-management scheme, which scales logarithmically with network size O (log n), with respect to storage space. 3. To provide two encryption and decryption standard. In Decryption using a private key set. 4. Key Management System provide at offline-line centralized server. 5.2 Problem Definition Let us assume a group of people in an incident area, who want to change correspondence securely among each other in a pair-wise fashion.2 The key pool of such a K group consists of a set of private–public key pairs, and is maintained by an offline trusted server. Each key pair consists of two mathematically related keys. The key pair in the key pool is represented by (k^i priv, K^i pub). To support secure communication in the group, Every member is loaded with all public keys of the group and assigned a distinct subset of private keys. 5.3 Module Description

Modules

1. User Registration

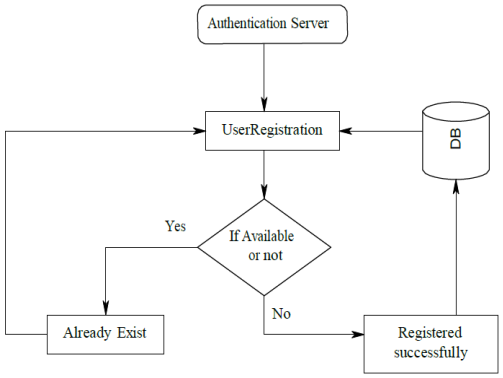
2. Key Allocations

3. Encryption

4. Decryption

1. User Registration: This Module is used to Register the user(node) information, such as User Name, Password, System name ,and port no in Authentication server. The all information's are stored in database. When the user registration, same user can not register more than one time. The unique user only allowed for key allocation.

Fig 2- User Registration



2. Key Allocations: In this module, we obtain key size, using key allocation algorithms. That is how many public keys and private keys allocated based on network size(number of user).After allocation keys, generate the distinct private keys sets those who are all registered Authentication server. Each user stored the common public keys and a own private key set.

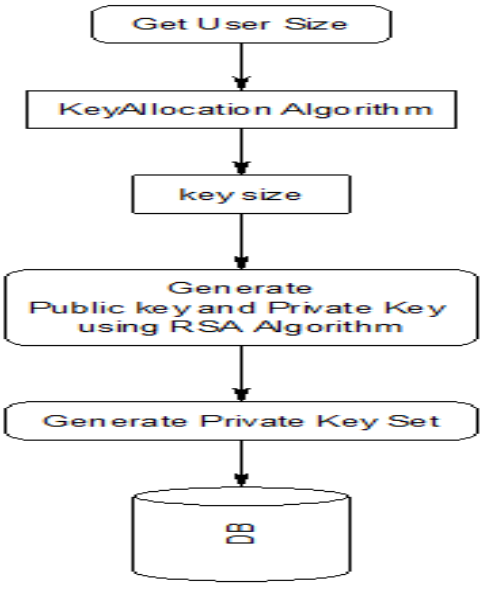


Fig 3- Key Allocation

3. Encryption: After stored keys in each User. Every user in mission critical environment is able to communicate securely with other user,

with the help of their stored keys. Before encryption, the user to make a request ID (Binary value).Here, the sending message would be encrypted using public key one, and then cyber text is encrypted one more time using public key two. Finally the message is transmitted to destination user

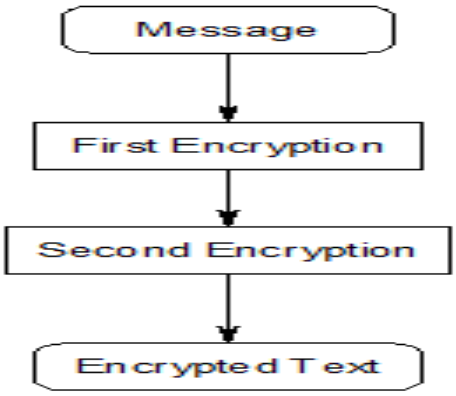


Figure 4: Encryption

4. Decryption: In this module, Decrypt message using already stored private keys set. First Decrypt the message using private key one and then to make another decryption using second private key. Finally we can show message in receiver text area.

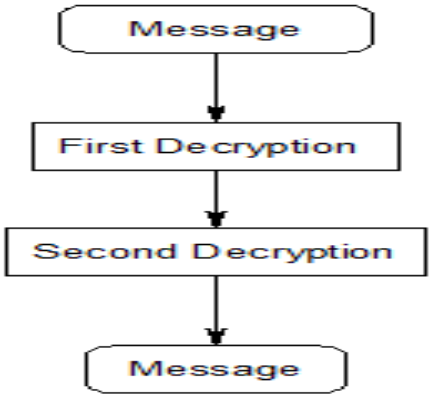


Fig -5: Decryption

System Architecture:

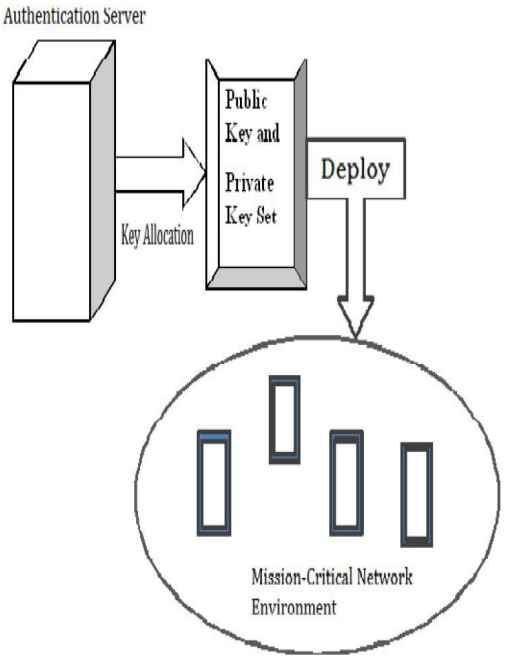


Fig- 6: System Architecture

Conclusion

We generate a key-management scheme, which requires significantly less key storage space than traditional schemes and almost zero communication overhead for authentication in wireless mission-critical network with nodes. We have generalized the traditional public-key-management schemes. And location based key management system turned out to be the traditional public-key infrastructure. We can also see that in Location Based Key Management Scheme For Wireless Mission-Critical Networks fulfills the secure communication requirements in terms of integrity, non-repudiation, and service availability.

References:

[1]Wenbo He ¤ Ying Huangy, Ravishankar Sathyam, Klara Nahrstedty , Whay C. Leez , "SMOCK: A ScalableMethod of CryptographicKey Management for Mission-critical Wireless Ad Hoc Networks ", IEEE transactions on information forensics and security, vol. 4, no. 1, march 2009 .

[2] Wenbo He, Ying Huang, Klara Nahrstedt ,Whay C. Lee , "SMOCK: A ScalableMethod of CryptographicKey Management For Mission-Critical Networks.