ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

A Novel Approach of Management for Mission-Critical Wireless Ad-Hoc Network

S.Elakkiya[1], H.Lookman Sithic[2]

Research Scholar, Muthayammal College of Arts & Science, Namakkal, Tamilnadu, India[1]

Associate Professor, Dept. of Computer Applications, Muthayammal College of Arts & Science, Namakkal, Tamilnadu, India[2]

ABSTRACT: In Mission-critical networks it shows great potential in emergency response and /or data recovery, health care, critical in-restructure monitoring, analyzing etc. Such mission-critical applications demand that security service be "anywhere," "anytime," and "anyhow." However, it is challenging to design a key management scheme in current mission-critical networks to fulfill the required attributes of secure communications, such as data integrity, authentication, secret, no repudiation, and service availability. In our work, we present a self-contained public key-management and private key scheme, a scalable method of cryptographic key management with encryption and decryption, which achieves almost zero communication overhead for authentication, and offers high service availability. In our scheme, a small number of cryptographic keys are stored offline at individual nodes before they are deployed in the network. To provide good scalability in terms of the number of nodes and storage space, we utilize a combinatorial design of public-private key pairs, which means nodes combine more than one key pair to encrypt and decrypt messages.

KEYWORDS: Cryptography; Management; wireless; Ad-hoc network; fuzzy logic

I. INTRODUCTION

The advances in cost-effective sensing, computing, and communication wireless devices, current mission critical systems are composed of mobile, autonomous, and wireless devices. Examples can be found in health-care (assisted living) systems, automotive networks, first responder systems (emergency rescue and disaster recovery), military applications, critical infrastructure monitoring, and so on. In these systems, it is important to support secure communications with the following attributes, data integrity, authentication, secret, non repudiation, and service availability. To build a secure communication system, usually the first attempt is to employ cryptographic keys. However, cryptographic key management is challenging due to the following characteristics of wireless ad-hoc communications.

1) Unreliable data communications and low bandwidth: due to the shared-medium nature of wireless links, data flows may frequently interfere with each other. Moreover, a network may be partitioned frequently due to node mobility and poor channel condition. Therefore, the communication overhead for a authenticate exchange cannot be ignored.
2) Network dynamics: mobile nodes may leave and join the ad-hoc network frequently and new legitimated nodes may join the network later after some nodes have been recruited in the field. Mobility increases the complexity for trust management.
3) Large scalability: the number of ad-hoc wireless devices deployed at an incident scene depends on the various nature of the incident. In general, the network size can be very large. In addition, an ad-hoc network should be able to accommodate more mobile devices if necessary; therefore, it is necessary to have newly deployed devices and previously deployed devices trust each other without introducing too much overhead.
4) Technical constraints: the wireless devices usually have limited bandwidth, memory, and processing power. Among these constraints, communication bandwidth consumption and memory are two big concerns for key-management schemes. Wireless bandwidth is the scarcest resource in a wireless network. On the other hand,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Memory concern for key storage is more evident, since the requirement on network scalability (or network size) is increasing.

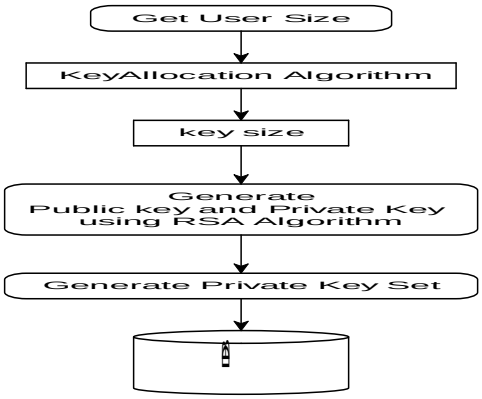
A. *Module Description*

- 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. The admin registration, same admin cannot register more than one time. The unique User only allowed for key allocation.

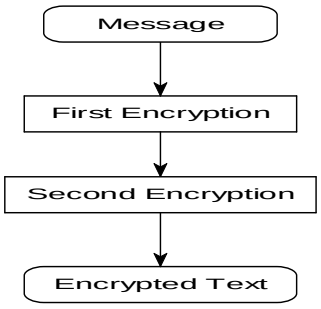
- Key Allocations

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



- Encryption

After every stored keys in each application. 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 to the user whom is going to send message. After that, the public keys would be getting for Encryption based on receiver 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.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

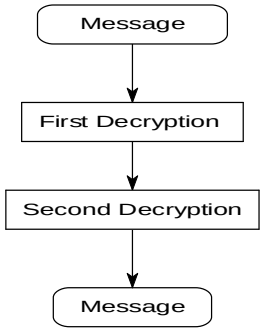
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

- 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.



II. RELATED WORKS

Akbani *et al.*, have proposed a hop-by-hop, proficient authentication protocol, called HEAP. It authenticates packets at each hop using a modified HMAC-based algorithm including two keys and drops any packets that are initialized from outsiders. The method used here can be appropriate for all application like multicast, unicast or broadcast applications. Discovering an insider attack using this protocol is highly improbable. But if a third party Intrusion Detection System (IDS) happens to detect a compromised insider node and raise an alarm to other nodes, HEAP will offer a framework for an effective response system.

Wenbo *et al.*, have proposed a self-contained public key-management scheme, a Scalable Means of Cryptographic Key management, which acquires negligible communication overhead for authentication, and offers maximum service availability. Here a combinatorial design of public private key pairs is created which provides each node with extra protection of more than one key pair to encrypt and decrypt messages. This format helps in earning higher stability in terms of nodes and storage space. The scheme also achieves controllable resilience against node compromise by defining required benchmark resilience.

Saxena *et al.*, have discussed about various signature scheme and have studied about the various techniques used. Here they tried the threshold in constructing decentralized access control mechanisms for ad hoc groups. They tried to first, point out the drawbacks of known threshold RSA signatures and tried to build access control mechanisms based on a variety of flavors of distinct logarithm based threshold signatures in this paper they tried to implement three access control mechanisms based on discrete-logarithm based threshold signatures, Threshold DSA (TS-DSA), Threshold Schnorr (TS-Sch) and Threshold BLS (TSBLS).

III. PROBLEM DEFINITION

A. *Existing Systems*

In secure communication, wireless sensor networks use symmetric key techniques. In symmetric key techniques, secret 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 authentication - based approaches were originally proposed to provide solutions to secure communications for the Internet, where security services rely on a centralized authentication server. The authentications -based approaches to ad-hoc networks and present a distributed public-key-management scheme for ad-hoc networks, where

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

multiple distributed authentication authorities are used. To sign a authentication, each authority generates a partial signature for the authentication submits the partial signature to a coordinator that calculates the signature from the partial signatures.

❖ *Disadvantage*

- Lack of support for authentication and secrecy.
- Total number of keys held by each user is traditional key-management schemes
- Multiple-point failure of the centralized server is able to paralyze the whole network, which makes the network extremely vulnerable to compromises and denial-of-service attacks.

B. *Proposed System*

In this system we propose to support secure communications with the attributes of data integrity, authentication, secrecy, non repudiation, and service availability. To build a secure communication system, usually the first attempt is to employ cryptographic keys. In, let us assume a group of people in an incident area, who want to exchange correspondence securely among each other in a pair-wise fashion.2 .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 first key pair in the key pool is represented. To support secure communication in the group, each member is loaded with all public keys of the group and assigned a distinct subset of private keys. Each 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.

❖ *Advantage*

- To Support secure communications among the users in Mission-Critical Wireless Ad-Hoc Networks.
- In the management scheme, which scales logarithmically with network size O (log n), with respect to storage space.
- To provide two encryption and decryption standard.
- Key Management System provide at offline-line centralized server.
- Problem Formulation

Let us assume a group of people in an incident area, who want to exchange 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 first key pair in the key pool is represented. To support secure communication in the group, each member is loaded with all public keys of the group and assigned a distinct subset of private keys.

IV. CRYPTOGRAPHIC ALGORITHMS

One of the foremost challenges is the mismatch between the energy and performance requirements of security processing. In this paper energy consumption of the security protocols and cryptographic algorithms are assured. Symmetric algorithm use same key for encryption and decryption. Asymmetric algorithm uses public and private key for encryption and decryption. Hash algorithm takes a message of arbitrary length and outputs a fixed-length hash number representative of the message. Even a minor change in the original message can result in the computation of a different hash value.

Asymmetric algorithm consumes energy for key generation, signature and verification. RSA utilizes minimal energy for verification, while Digital Signature Algorithm consumes more energy. Hash algorithms are the least complex of the cryptographic algorithms and should intuitively incur the least energy cost.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Node A sends Request to node(s) B.

- *If* node A has direct trust value on C, then it will reply back with response.
- *Else If* A does not have direct trust value record it will discard the request
- After receiving request reply from neighbours consider the trust value of the
- Node with maximum direct trust value by applying fuzzy logic.
- Integrate all the obtained RT value from neighbours to calculate the indirect trust value

Where

- Respond is Recommendation Trust Request.
- Respond is Recommendation Trust Reply

Where,

- FT value = Final Trust Value of Node
- E value = Energy Value of Node
- T value = Trust Value of Node
- PIC value = Packet-Integrity Value of Node

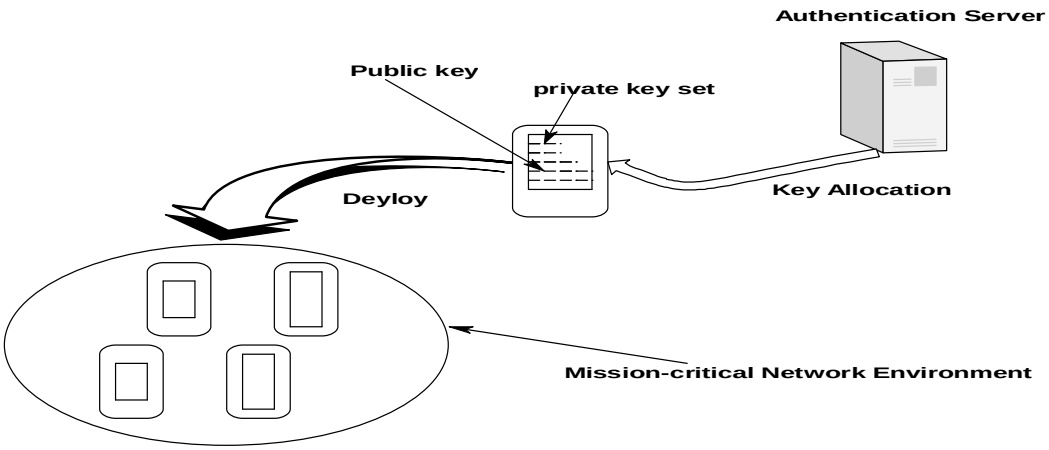


Fig 1. Architecture for Mission-Critical Network Environment

A. *Fuzzy Based Analyzer*

Trust level represents a node's behaviour for reliability where the positive experiences increase the trust level of the node and negative experiences decrements the trust level. Fuzzy logic provides ability to handle uncertainty and imprecision effectively. Fuzzy logic based algorithm for trust has been devised and it is applied to the calculated trust value of the nodes. Trust values are computed based on E value, T value, PIC value produce FT value. These values are treated as fuzzy input variables and the Fuzzy logic based algorithm marks the nodes as either trusted or malicious. Fuzzy logic based algorithm will be called when the nodes request Certificate Authority (CA node) for certificates to exchange data packets. A two way Fuzzy based analyser has been designed based on trust values, either to be trusted for data exchanges or marked as malicious if it falls below a Critical threshold and its isolated from the network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Simulation System Parameters	
Parameter	Default Values
Routing protocol	AODV
Simulation time	1 min
No of nodes	6
Mobility Model	Random Waypoint
Traffic type	CBR
Payload size	512 bytes
`ISAKMP	Enable

Fig 2. Simulation Parameter

V. IMPLEMENTATION

Implementation is the stage in the project where the theoretical design is turned into a working system and is giving confidence on the new system for the users, which it will work efficiently and effectively. It involves careful planning, investigation of the current System and its constraints on implementation, design of methods to achieve the change over, an evaluation, of change over methods. Apart from planning major task of preparing the implementation are education and training of users. The more complex system being implemented, the more involved will be the system analysis and the design effort required just for implementation.

An implementation co-ordination committee based on policies of individual organization has been appointed. The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out, discussions made regarding the equipment and resources and the additional equipment has to be acquired to implement the new system. Implementation is the final and important phase, the most critical stage in achieving a successful new system and in giving the users confidence. That the new system will work is effective .The system can be implemented only after through testing is done and if it found to working according to the specification. This method also offers the greatest security since the old system can take over if the errors are found or inability to handle certain type of transactions while using the new system. We implemented under the context of the trustworthy cyber infrastructure for the power grid (TCIP), with C language in the Linux operation system. In our implementation, nodes receive 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 wants to send a message to another node (the receiver), it 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 then encrypt the message by using the receiver's keys. And the receiver can then decrypt the message using its private keys. We measured the encryption and decryption process time that was taken to encrypt and decrypt a message.

VI. CONCLUSION

We depict a self-contained key-management scheme, which requires especially it can less key storage space than traditional schemes and almost zero communication overhead for authentication in a mission-critical wireless ad-hoc network with nodes. The scheme also achieves controllable resilience against node compromise by determining required benchmark resilience. We generalized the traditional public-key-management schemes. In this it turned out to be the traditional public-key infrastructure. We can also see that fulfills the secure communication requirements in terms of integrity, authentication, secrecy, none determining, and service availability.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Trust is assigned to all the mobile nodes considering the available energy and the nodes are clocked and time lined. Centralized system will monitor the trusted nodes and malicious nodes and assures the certificate exchange is only to trusted nodes. Certificate Authority will protect the data exchange by allowing the trusted entities to participate in the network, isolating the malicious nodes. Trust can alone provide a trustworthiness value of node in a precise way. Fuzzy Logic based on Certificate Authority will provide secure way of message exchanges. Integrated approach of Trust and Fuzzy logic based Certificate Authority will secure the communication.

REFERENCES

1. M Rajesh Babu, Selvan S,(2010) "A Lightweight and Attack Resisitant Authenticated Routing Protocol For Mobile Adhoc Networks", International Journal of Wireless &Mobile Networks(IJWMN), Vol.2, No.2.
2. A.Rajaram and Dr.S.Palaniswami , (2010), "Detecting Malicious Node in MANET using trust based Cross-Layer Security Protocol", International Journal of Computer Science and Information Technologies,Vol 1(2).2010 Pg No:130-137
3. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proc. 10th ACM Conf. Computer and Communications Security, Oct. 2003
4. D. Boneh and M. Franklin, "Identity based encryption from the Weil Pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.
5. D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure For key distribution in TinyOS based on elliptic curve cryptography," presented at the 1st IEEE Int. Conf. Sensor and Ad Hoc Communications and Networks, Santa Clara, CA, Oct. 2004.
6. G.S. Mamatha and Dr. S. C. Sharma , (2010) "A Highly Secured Approach against Attacks",International Journal of Computer Theory and Engineering, Vol. 2, No. 5.
7. Cheriton, D and Skeen, D. Understanding the Limitations of Causal and Totally Ordered Communications. *Proc 13th SOSP*, Ashville, N.C. Dec. 1993 (44-57).
8. Demers, A. *et. al.* Epidemic Algorithms for Replicated Data Management. *Proceedings of the 6th Symposium on Principles of Distributed Computing (PODC)*, Vancouver, Aug. 1987, 1-12.
9. Floyd, S., Jacobson, V., McCanne, S. Liu, C., and Zhang, L.. A Reliable Multicast Framework for Lightweight Sessions and Application Level Framing. In *Proc SIGCOMM `95*, Aug. 1995.
10. J. Gray, P. Helland, P. O'Neil and D. Shasha. The dangers of replication and a solution. *Proceedings 1996 SIGMOD Conference*, June 1996.
11. Richard Golding and Kim Taylor. Group Membership in the Epidemic Style. Technical report UCSC-CRL-92-13, University of California at Santa Cruz, May 1992.

BIOGRAPHY

Miss S.Elakkiya, She has received her B.Sc (CS) from Muthayammal College of arts and science, Rasipuram and M.Sc from Muthayammal College of arts and science, Rasipuram. She is pursuing M.Phil Muthayammal collage of arts and science, Rasipuram.

MR.H. Lookman Sithic M.Sc.IT., M Phil., Associate Professor, Department of computer Application, 1999 B.Sc Jamal Mohammad College Trichy, 2001 MS(IT) Jamal Mohammad College Trichy, 2004 M Phil-PRIDE Periyer University.