A SECURE KEY MANAGEMENT SCHEMES FOR IMPROVING THE ENERGY EFFICIENCY OF MANET

Mukesh Kumar
The Glocal University, Mirzapur, Saharanpur, UP, India

Abstract

Infrastructure less network is MANET which creates the temporary network. Performance and security are its two major issues. Due to its self organizing feature providing runtime network security is tedious task. MANET has been developed as a platform for controlling the applications. Privacy and authentication expands the key management for securing MANET. Due to its dynamic nature of efficient framework for securing the networks a symmetric key establishment is considered. Though MANET is efficient with dynamic infrastructures they are related to various security risks . In this paper , we have proposed Security key management (SKM) paradigm to provide authenticity over information for MANET. It shows Dispense Key method for generation and distribution of the keys. Then compared out framework Security key management (SKM) with our proposed algorithm and Advance Encryption Standard (AES) ,RSA, DES and shown the increased scalability of our framework.

Keywords: SKM; Symmetric; Asymmetric, Manet, Key Generatio

I. INTRODUCTION

Wireless Manet is a new infrastructures less communication technology which is proposed of those conditions where management of infrastructure costs high. Apart from this merit it has demerits in terms of secure communication. Manet is defined by its features like self-organizing, distributed application and multi node routing. Due to its dynamic nature maintaining the secured communication is tedious when centralized management does not exist. In such condition key management schemes can achieved the secure communication .Their schemes depends on certificate based cryptography (CBC) where the certificate issue authority uses ID based cryptography to generate the certificate. Gary C. Kessler has proposed this scheme in his work for secured communication. Other is Identity based cryptography .In this scheme a publicly known key is representing an organization and used as public key. The practical implementation of this scheme is done by Sakai in 2000. ID based schemes removes the requirement of certificate based public key distribution. It enables any two trustworthy user to communicate securely without sharing the certificate which is managed by private key generators. In this paper we have proposed a Security Key management approach for the security of information over MANET where our proposed algorithm is attached with the security key management dispense key for the generation of keys and its distribution concerning with high performance for secure authentication.

PROBLEM DEFINITION

In this paper, we have proposed a method for secure information sharing over MANET by secure key management schemes. In this proposed method we have analyze McEliece Algorithm and then attached with our key generation method for distributing the keys. Our proposed method will help to minimize the required time for encryption and decryption of data by number of keys reduction. Secure authentication mechanism is provided by our method approach. Our Security protocol based on our proposed method and provide the high security and minimum computational complexity.

II. RELATED WORK

Key management schemes on MANET are classified into three types

Centralized Schemes

Decentralized Schemes

Distributed Schemes

In centralized schemes, a key manager node is responsible of key management for reliable end to end communication

In decentralized schemes , the entire network is divided into managing layer by n(n-1)/2 and each layer a member is selected randomly as a group leader.

In distributed method, all network cooperates to implement a key protocol.

Jian Zhou et al. proposed a delay tolerating network (DTN) where in a binary tree like structure where one encryption key and multiple decryption key protocol operates the networks.

Zhang and Wang[6] has given a certificate –less effective key management (CL-EKM) that upgrades key generation for secure communication channel. The keys in CL-EKM uses set wise node communication. Manhattan mobility model for simulation of nodes is an example. In this method Sumanthy and Kumar[4] has shown that after computing number of nodes and distance between the nodes a key is generated to transform the messages where key is exchanged between the receivers. Key and message in encrypted form is encapsulated. Figure 1.1 shows the this model.

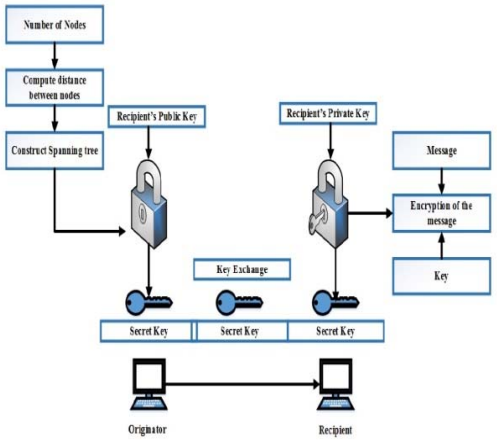

Figure 1.1 Key management architecture

Franklin et all[1] presented fully implemented and efficient secure Identity based encryption(IBE) scheme in 2001. Lynn et all[2] used the same approach using paring . This scheme represents that the receiver can share sender a public key to encrypt the message and PKG provide a private key to decrypt the ciphertext by the receiver. CK.Kaya et all[3] has proposed a secret scheme for secure data transmission using CRT. But cost of computation exceeds due to the modular security. A protocol

(JRSS) has proposed to authenticate the secret sharing. The security of this method is used by CRT method. NIkolay an American mathematician proposed a model for data transfer development in MANET with CRT scheme where threshold secret sharing schemes (SSS) acquiring the computation capability . In order to reduce the computational complexity the author[4][5] proposed a group key handling schemes using CRT. Mare Joye et all[6] proposed a group key handling scheme to reduce the computational complexity where the CRT reduces the key combination to generate the key over server. Cui et al[5] proposed the Usage Based Key Management[7] (UBKM) protocol to avoid the selected nodes from security attacks for authentication using encryption by one – way hash function. But when various messages are exchanged over MANET single key mechanism is not appropriate. UBKM protocol rectify the above mentioned issues. Yao et al[7] proposed a LKH++ based low power group key management for MANET security . It works firstly by constructing a secure tree . This method includes two phase first to construct a tree and secondly to hold the keys . But results has shown increasing level of security but less computation overhead. Boa et al[8] proposed a method to overcome from the issues such as scalability and communication overhead by using group based key management schemes in clusters of MANET . Results has shown overhead reduction in energy and time consumption.

Qin et al.[9] proposed a method for key management applied on Elliptic Curve Cryptography (ECC) and AVL tree for resolving the security problems. For maintaining of information they have proposed Elliptic Curve Peillier Encryption (ECPE) . As a result the security was improved due to periodic updates of the keys.

Yu-Li and Lin[10] has proposed the key management method for dynamic hierarchical access control based on ECC where group of nodes considered as class where each nodes information is maintained . Every class contains security key which is partially in ordered relation.

El-Din et al.[11] proposed a security framework based on energy efficient schemes to save energy named as Virtual ECC group key. This framework overcomes from the problem of computational cost, memory availability and overhead in communication.

Another scheme for efficient key management wry less memory and computation task has been proposed by Reddy et al[12]. In this scheme vandermonde matrix is used to generate the keys which is consider to be prone to attacks . In this scheme each node contain column for pulci information of node and row for secretly calculated key generation. But problem was to maintain column and row information of nodes as MANET is a huge network.

Vijay Kumar et al.[13] has proposed a Unified Key Management function (UKMF) which works across multiple protocols within the same network layer . This UKMF is a ciphering mechanism across all the network protocols. Figure shows abstract model of the proposed method ,which refers to the application layer and data link layer protocols.

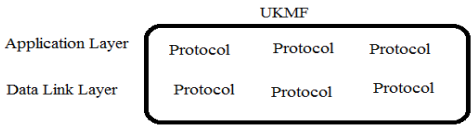

Figure 1.2 : Conceptual Model of Key management

Proposed Method
In this research work we have proposed a method which contains the method for Security key management with three functions as follows
Key generation Key distribution Key analysis

For the above part implementation we have used the centralized scheme of wireless network where all the above three key operations are managed by the centralized server For applying our SKM scheme initially due to large number of nodes in MANET clustering is required first.

III. CLUSTERING THE NODES

To maintain confidentiality in data cryptographic methods has to be applied. In our method nodes of MANET are equally grouped in to cluster and cluster head of each is appointed on the basis of any higher energy node. This Cluster Head will be considering as a cluster controller for managing overall Security key management schemes for key generation. Cluster Head is responsible which again shows mutual agreement between cluster head with others clusters for distribution.

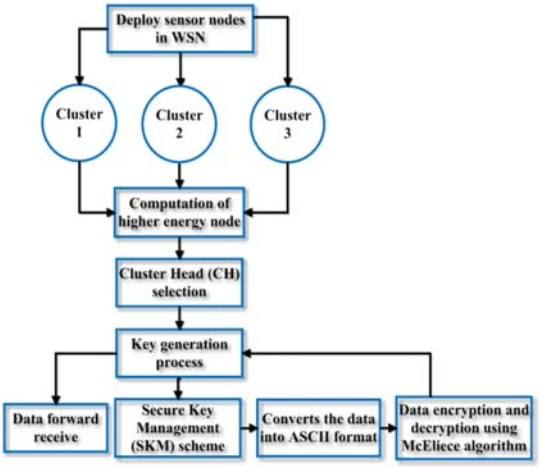

Figure 1.3: Overall Process of SKM scheme

Cluster Head Selection
A node in a cluster with more processing power , high energy and large memory is eligible for the Cluster head selection.
Selecting a CH by the controller consists of following steps

Step-1 Based on the node parameters in a cluster , each of node is tested for eligibility.

Step-2 Any node having more than 25% of energy can be eligible for CH

Step-3 Among all the eligible nodes higher energy nodes is selected for CH.

IV. SECURITY KEY MANAGEMENT

Securing the network by keys results the reduction in complexity if the network. These keys are secured by symmetric leys method. Minimizing the secure key management scheme

was proposed. While transferring of the data in a secure channel following steps are performed

V. KEY GENERATION

Master keys may be distributed till the network life . These keys are produced by servers which are pre distributed to the sensor nodes. At regular intervals key generators generates various new keys. Hamming code technique are used for data encryption by using keys.

Hamming code uses a matrix M with n X k dimension matrix. Error detection and rectification are also done by hamming code. Parity addition also do the rectification of error. Error code representation in matrix form is denoted as [n,k,d], where n show length of code,n is minimum distance , k is dimension of matrix . For example , if a hamming code is represent as (5,6,8) its algebraic curve in a finite area is used to form a linear code as follows

Step-1 a Matrix M with k X k dimension
Step- 2 Second matrix P with n X n dimension is assumed
Step-3 Calculate G'=G X M X P;
Step-4 Public key are computed in matrix order keys are estimated.

Key Distribution

After keys generation distribution of keys are given to the selected nodes where master keys encrypts the new keys. Distribution of keys always takes place in an organized order.

Proposed Algorithm for Key Encryption and Decryption

This Algorithm is applied for Encryption and Decryption of information which steps are as follows

Step-1 Plaintext P is considered , which is added with weight vector e.
Step-2: Cipher text C is calculated as
C=P*M+e
Step-3 Encrypt text is form by following expression
C=P*M+e

Process of Decryption

Step-1: Decryption is applied by taking first six components of encrypted text y1 , which is represented by Y0.
Step-2: Plaintext should be calculated as

X=S-1 * y1

Distribution of keys is applied over nodes and is done by Dispense Key method.

Dispense Key method

Exchanging the keys in a set wise method for a cluster is done by Dispense Key method.

A pool is maintained by a trusted server to maintain a record of public and private keys. Pair of public and private pair of keys maintains under a set by (Kipriv,Kipub). Their expression are denoted by Ipriv and Ipub.

It works when sender sends a secret message to the receiver node, that sends should be aware of Kpub and Kipr for anonymous receive Encryption by the sender is done with Kpub and then forwards to the receiver . Receiver open the message using private key Kipr.

For ex: In a cluster 8 nodes secure communication can be shown by
1(K1pr,K1pu),
2(K2pr,K2pu),3(K3pr,K3pu),4(K4pr,K4pu)
In this example cluster controller hold 4 public keys and 2 private keys. Public key should be shared by all nodes but private key will be shared within appropriate node.

VI. RESULT AND ANALYSIS

The result is done by using java JDK 1.7. The IDE Netbeans 6.9.10 and MySql for backend database.

For Deploying SKM following simulation parameters are used

Table : 1.1

Parameters	**Values**
Number of nodes	10,20,30,40,50
Simulation time	300 Seconds
Area	500X500
Number of cluster	4
Key size	1024 Bits
File size	256,512,2048

Execution Time for Encryption

The SKM efficiency is an authentication against the techniques like AES, DES and RSA. Parameters we have used are as follows

- Total time for Encryption and Decryption
- Memory consumption by the existing algorithm for Encryption and Decryption.

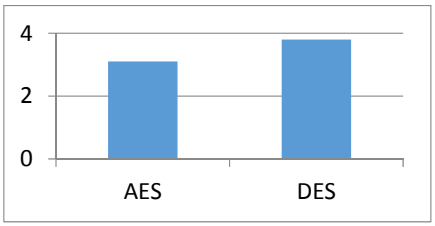

Figure 1.4 Comparison of Execution Time(Encryption) for

AES and DES

The execution time for our proposed method is validating against existing AES, DES and RSA when compared provides less time of execution for encryption.

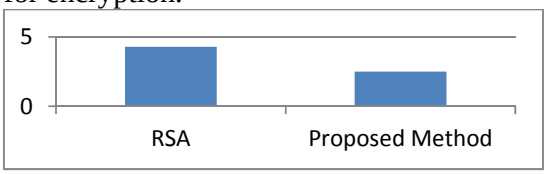

Figure 1.5 : Comparison of Execution Time (Encryption)

for RSA and Proposed Method

Advantages of Proposed Algorithm

- Key length of DES Algorithm is 266 bits and AES also 266. So number of rounds required for generation encryption is more.
- Key length of both RSA and our proposed method is 1024 bits. In spite of equal number of rounds for encryption process our proposed method consumes less time of execution for encryption due to the less number of rounds.

VII. CONCLUSION AND SCOPE OF FUTURE WORK

Most of the security algorithm are not suitable for MANET due to its dynamic nature. For ensuring security SKM technique is proposed which uses Dispense key approach effective of key generation. Due to the large key size our proposed method provides high secure authentication. Our Future work includes the memory consumption during Encryption and Decryption Time.

References:

[1] M. Panda, "Security Threats at Each Layer of Wireless Sensor Networks," International Journal of Advanced Research in Computer Science and Software Engineering, 3, 2013, 61-67.

[2] H. Delfs and H. Knebl, "Symmetric-Key Cryptography," in Introduction to Cryptography: Principles and Applications, ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, 11-48.

[3] X. Zhang and J. Wang, "An efficient key management scheme inhierarchical wireless sensor networks," in Computing, Communication and Security (ICCCS), 2015 International Conference on, 2015, 1-7.

[4] B. Cui, Z. Wang, T. Guo, G. Dong, and B. Zhao, "UBKM: A Usage-Based Key Management Protocol for Distributed Sensor Networks," in Emerging Intelligent Data and Web Technologies (EIDWT), 2013 Fourth International Conference on, 2013, 267-272.

[5] J.-Y. Huang, I.-E. Liao, and H.-W. Tang, "A forward authentication key management scheme for heterogeneous sensor networks," EURASIP Journal on Wireless Communications and Networking, 2011,

[6] 6. Z. Wang, X. Du, and Y. Sun, "Group key management scheme based on proxy re-cryptography for near-space network," in International Conference on Network Computing and Information Security (NCIS), 2011, 52-56.

[7] W. Yao, S. Han, and X. Li, "LKH based group key management scheme for wireless sensor network," Wireless Personal Communications, 83, 2015, 3057-3073.

[8] 8. X. Bao, J. Liu, L. She, and S. Zhang, "A key management scheme based on grouping within cluster," in Intelligent Control and Automation (WCICA), 2014 11th World Congress on, 2014, 3455-3460.

[9] Z. Qin, X. Zhang, K. Feng, Q. Zhang, and J. Huang, "An Efficient Key Management Scheme Based on ECC and AVL Tree for Large Scale Wireless Sensor Networks," International Journal of Distributed Sensor Networks, 2015.

[10] 10. Y. Zang, J. P. Thomas, G. Ghinea, M. Thomas, and S. Darwish, "Secure Sector Based Bi-path Clustering and Routing Protocol for WSNs," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012, 777-784.

[11] A. E. El-Din, R. A. Ramadan, and M. B. Fayek, "VEGK: Virtual ECC

group key for wireless sensor networks," in Computing, Networking and

157 Communications (ICNC), 2013 International Conference on, 2013, 364-368.

[12] R. S. Reddy, "Key Management in Wireless Sensor Networks Using a Modified Blom Scheme," arXiv preprint arXiv:1103.5712, 2011, 1-9.

[13] M. Vijayakumar, V. P. Dharshini, and C. Selvan, "A New Key Management Paradigm for Fast Transmission in Remote Co-operative Groups," International Journal of Computer Science and Mobile Computing, 3, 2014, 197-201.