A Framework to improve the Network Security with Less Mobility in MANET

Inderpreet Kaur
Research Scholar,
Mewar University,
Chittorgarh,
Rajasthan, India

A. L. N. Rao, PhD
HOD IT Department
G.I Bajaj Greater Noida
India

ABSTRACT
Infrastructures 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. So an efficient and strong model is required to setup so that various eavesdropping activity can be avoided. Key management is a vital part of security in Manet because the distribution of encryption keys in an authentication manner is a difficult task due to its dynamic nature. As every time nodes leaves or joins it has to regenerate a new session key for maintaining secrecy. In this paper, we have proposed a new key management scheme to improve the network security with less mobility overhead and less key distribution time .

Keywords
Manet, certificate based cryptography , symmetric keys.

1. INTRODUCTION
Wireless Manet is a new infrastructure less communication technology which is consists 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 is a difficult task to achieve a secure communication. Using managing of secure key distribution for security speed varies w.r.t applications. For example in military based application it will take ling time due to long range network but in commercial applications it will take a short time due to short distance. So we can say speed is inversely proportional to network range. In key management schemes different cryptographic keys method are used like symmetric keys, public keys or certificate based cryptography. In symmetric keys over MANET if n nodes wants to communicate k keys will be required where k will be the number of leys which should be generated by **k=n(n-1)/2.** In this approach both the sender and the receiver contains the same key for encryption and for decryption. In public key encryption two keys are used one private key and the other as public key. The private keys are used for encryption between the nodes whereas public keys are used for encryption .Their schemes depend 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 new key management scheme to improve the network security with less mobility overhead and less key distribution time . The rest of the paper is organized as Section II related work Section III overview of key management schemes Section IV Proposed method Section V Results Section VI conclusion

2. RELATED WORK
Key management in MANET is getting popularity for researchers . Shamir et all[1], has proposed ID based public key systems which uses user's identity for secure information transmission . ID based systems exchanges the public key certificates without keeping public key directory. This method needs a Private key generator (PKG) to identify user id . Identity based key management schemes are further classified as

1. Traditional threshold schemes
2. Hierarchical identity based schemes
3. Secret share as private key (SSPK)
4. Certificates schemes

Franklin et all[2] presented fully implemented and efficient secure Identity based encryption(IBE) scheme in 2001. Lynn et all[3] 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. Some of the algorithms[4] are specified based on IBE . Figure 1 illustrates the IBE scheme.

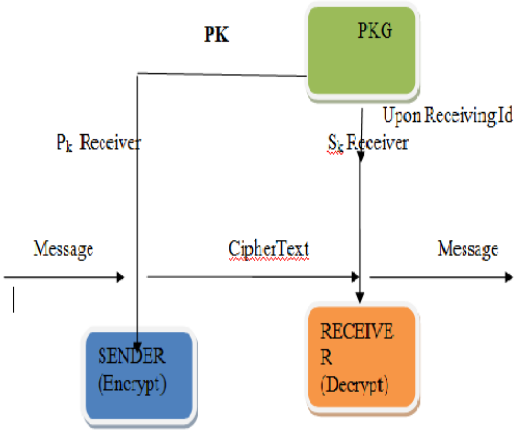


Fig 1: Working of IBE System

Unlike Identity based encryption for securing MANET various schemes based on Chinese remainder theorem has been proposed and implemented. Sarkar et all[5] has proposed a new RSA threshold secure MANET based on Chinese remainder theorem. CK.Kaya et all[6] 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[7][9] proposed a group key handling schemes using CRT. Mare Joye et all[8] proposed a group key handling scheme to reduce the computational complexity where the CRT reduces the key combination to generate the key over server.

3. KEY MANAGEMENT SCHEME

Various key management scheme has been proposed using the number of distribution procedures. Various Symmetric key management schemes like Key Infection , Peer intermediate key establishment. Some of the Asymmetric key management schemes are secure routing protocol , Ubiquitous and robust Access but these schemes includes the parameters like

- **Increasing Security** – Reducing small calculations will consume less computation node power to improve network security.
- **Expanding Mobility** - computational procedures can be reduced by decreasing the allocation of resources to extend mobility.
- **Reducing key generation time**- Network quality can be improved if key generation time can be reduced.
- **Reducing Power**- Due to the battery depended network , power conservation is important to improve the network consistency.

3.1 Proposed Key Management Scheme

Our proposed scheme consists of following tasks

1. **Removal of misbehaviour Node**: When system identified a Cluster head is misbehaving . Head of the cluster will be removed from table
2. **Key generation**: Based on CRT technique , after removal of misbehaviour node from table list the key generation will be applicable by the algorithm and it will be allowed to a node having a largest ID according to its time allocation in a network ,then all the members should be updated by this new head node.
3. **Cluster head verification:** When messages of key generation is received by other member nodes the details about the Node ID will be recorded in its table. And also it is ensuring that no further interaction should be done with the node, which will implement a secured communication.
4. **Key Generation and Management Schemes:** Key Generation and Calculation of pair wise prime keys will be generated by calling a function. Key generation computation can be calculated in pairs, so that generation time should be reduced . It will also help to define that quality of the network .

   Let P1,P2,P3 _ _____Pn are prime integer values.

   Let integer values are a1,a2,a3_____a_n . It unique solution is

   X=ai(mod Pi)for 1<=i<=r

   which is given by

   X=a1M1X1 + a2M2X2 +_____$a_nM_nX_n$(mode M)

Algorithm

Step 1: Start

Step 2: Cluster head returns flag as 1 (indicating misbehaviour of cluster head)

Step 3: Runtime deletion operation for the removal of cluster head from list.

Step 4: Call Key_reinvokation() . Calculate pair of prime keys which affect Z (to assign new CH) and distribution of secret key.

Step 5: If(!Z) repeat step 2 to step 3 till keys are generated.

Step 6 return result

Step 7 EXIT

Function Definition of Key_reinvokation()

Function will implement Chinese Remainder theorem using reducing approach with a domain specification for integers values

Assume t and U be positive prime numbers with a and b as integers

Such that N=a(mod t)

N=b(mod U)

N consists modulo till such that (t,U)=1, then every pair of residue modulo t and U corresponds to a simple remainder modulo t ,U

For i=1_____r mi are (set of congruence are)

$$X \equiv a_1 b_1 \frac{M}{m_1} + \cdots + a_r b_r \frac{M}{m_r} \pmod{M}$$

$M=m_1m_2$_____m_r

4. PERFORMANCE ANALYSIS

The algorithm is implemented in NS2 simulator 5.0 for N number of nodes. Key management procedure and key_reinvokation() function is implemented in C++ using dynamic memeory allocation.

Parameters we have taken

- Number of nodes for communication
- Duration of simulation
- Radio frequency range
- Key Updation duration
- Setting up channel bandwidth 10Mbps
- Protocols TCP/HTTP/802.11
- Node Speed 0 to 50 M/s

Table 5.1 Simulation Settings

Parameters	Default Values
Topology	Grid
Number of nodes	36
Transmission range	100m
MAC Protocol	802.11
Packet Size	512 Byte
Packet Interval	100 packet/sec
Bandwidth	5Mbps
Probe message Interval	1sec
Simulation Time	200 Sec

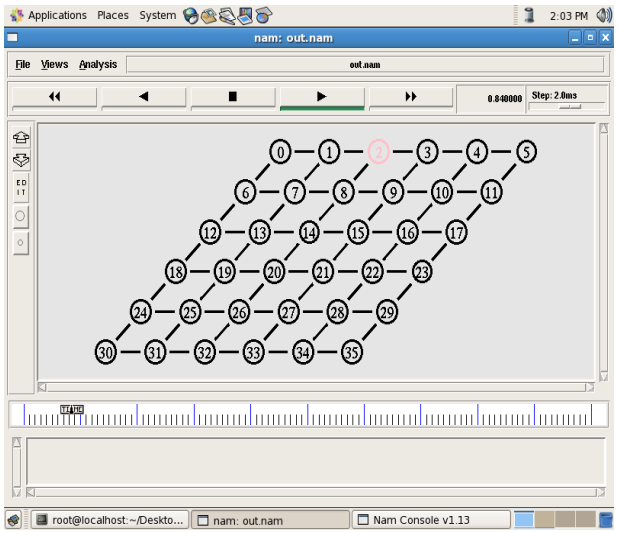


Figure 5.1 - Cluster Head selected as Misbehaviour Node

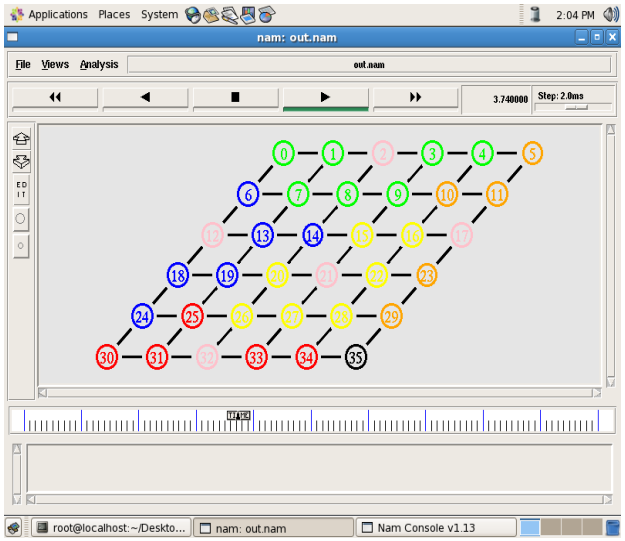
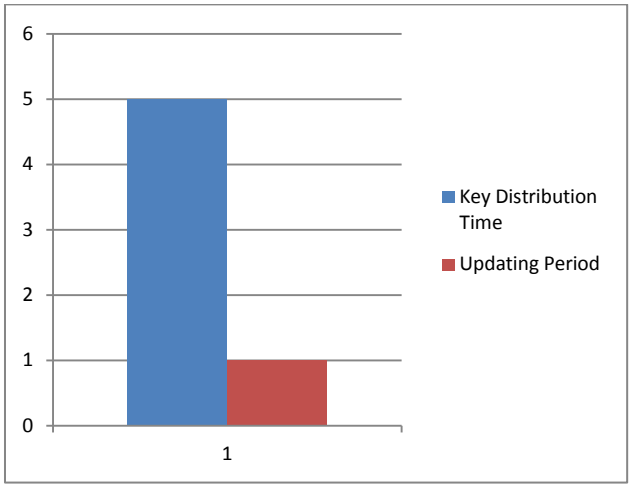


Figure 5.2 Key Generation using Key_reinvokation() by cluster head

S. No.	No. of keys Sent	No. of Key Received	Sending Time (sec)	Receiving Time (sec)
1	100	100	.00100	.00110
2	200	200	.00340	.00370
3	300	300	.00560	.00600
4	400	400	.06890	.07300
5	500	490	.12300	.12400
6	600	570	.16800	.16920
7	700	660	.20012	.20112
8	800	750	.21890	.22900

After having simulative analysis of the algorithm in C++ the proposed scheme performance on the key distribution time and Updating Period of cluster nodes is as follows



On the basis of the graph due to the efficient updating time of the keys over the nodes the proposed algorithm is an optimum solution.

5. REFERENCES

[1] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Adv. Cryptology—CRYPTO*, vol. 2139, New York, 2001, pp. 213-229.

[2] D. Boneh, B. Lynn, and H. Shacham, *Short Signatures From the Weil Pairing*, Gold Coast, Australia: Springer -Verlag, 2001, pp. 514-532.

[3] J. Baek, J. Newmarch, R. Safavi-Naini, and W. Susilo, "A survey of identity-based cryptography," in *Proc. 10th Annual Conf. for Australian Unix User's Group*, 2004, pp. 95-102.

[4] Sarkar,B.Kisku,S.Misra and M.S Obaidat " Chinese Remainder Theorem-Based RSA- Threshold Cryptography in MANET using Verifiable Secret Sharing Scheme" IEEE International Conference On Wireless and Mobile Computing, Networking and Communications,2009.

[5] CK.Kaya and A.A.Seluck, "A Verfiable Secret Sharing Scheme Based On the Chinese Remainder Theorem", DOCRYPT 2008,LNCS 5365.

[6] Marc Joye, Pascal Paillier, and Serge Vaudenay, "Efficient Generation of Prime Numbers," *CHES* 2000, vol. 1965 of LNCS, pp. 340-354, Springer-Verlag, 2000.

[7] Marc Joye, Pascal Paillier, and Serge Vaudenay, "Efficient Generation of Prime Numbers," *CHES* 2000, vol. 1965 of LNCS, pp. 340-354, Springer-Verlag, 2000.

[8] L. Huang, T. Lai, On the scalability of IEEE 802.11 ad hoc networks, in: ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), 2012, pp. 173–182.

[9] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao,and Chin- Feng Lai, Member, IEEE, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach ", IEEE systems journal, 2014.

[10] Elhadi M. Shakshuki, Nan King and Tarek R. Sheltami, " EAACK – A Secure Intrusion Detection System for MANETs "IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO.3, MARCH 2013.