International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

A Survey to Improve the Network Security with Less Mobility and Key Management in MANET

Ritu Aggarwal
MMEC, MULLANA Himalayan Group Of Professional Institutions, Kala Amb, Himachal Pradesh, India

ABSTRACT

Mobile ad hoc network (MANET) is now days become very famous due to their fixed infrastructure-less quality and dynamic nature. They contain a large number of nodes which are connected and communicated to each other in wireless nature. Mobile ad hoc network is a wireless technology that contains high mobility of nodes and does not depend on the background administrator for central authority, because they do not contain any infrastructure. Nodes of the MANET use radio wave for communication and having limited resources and limited computational power. The Topology of this network is changing very frequently because they are distributed in nature and self-configurable. Due to its wireless nature and lack of any central authority in the background, Mobile ad hoc networks are always vulnerable to some security issues and performance issues. The security imposes a huge impact on the performance of any network. Some of the security issues are black hole attack, flooding, wormhole attack etc. In this paper, we will discuss issues regarding low performance of Watchdog protocol used in the MANET and proposed an improved Watchdog mechanism, which is called by I-Watchdog protocol that overcomes the limitations of Watchdog protocol and gives high performance in terms of throughput, delay.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, AODV, Black Hole, RREP, RREQ, RRER, Malicious Node, Manet, Certificate Based Cryptography, Symmetric Keys

I. 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 loing 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 .

II. 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 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.[6] 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.

III. KEY MANAGEMENT SCHEME

Various key management scheme has been proposed using the number of distribution procedures. Various Symmetric key management schemes like Key Infection , [14]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.

IV. KEY MANAGEMENT IN MOBILE AD HOC NETWORKS

As an introduction to key management, this paper briefly considers the classification of security problems in MANETs. The aim is to position the problem of peer-to-peer key management within the MANET security field. The main observation is that cryptographic techniques are often at the center of solving security problems in MANETs and hence need key management . The subsequent subsections also provide definitions and terminology for the different properties and requirements of key management

4.1 **Defining Key Management** A keying relationship is the state wherein network nodes share keying material for use in cryptographic mechanisms.[15] The keying material can include public/private key pairs, secret keys, initialization parameters, and non-secret parameters supporting key management in various instances. Key management can be defined as a set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. In summary, key management integrates techniques and procedures to establish a service supporting. (1) initialization of system users within a network; (2) generation, distribution, and installation of keying material; (3) control over the use of keying material; (4) update, revocation, and destruction of keying material; (5) storage, backup/recovery, and archival of keying material, and (6) bootstrapping and maintenance of trust in keying material. Authentication is the basis of secure communication. Without a robust authentication mechanism in place, the remaining security goals (confidentiality, data integrity, and nonrepudiation) are in most instances not achievable. Authentication can only be realized by means of verifying something known to be associated with an identity. In the electronic domain, the owner of the identity must have a publicly verifiable secret associated with its identity; otherwise, the node can be impersonated. Authentication in general depends on the context of usage. Key management is concerned with the authenticity of the identities associated with the six services given above, it is a concept which may seem trivial at first, but one that is not easily achieved. Authentication of users is particularly difficult (and

in most network settings impossible) without the help of a trusted authority. The fundamental function of key management schemes is the establishment of keying material. Key establishment can be subdivided into key agreement and key transport .[16] Key agreement allows two or more parties to derive shared keying material as a function of information contributed by, or associated with, each of the protocol participants, such that no party can predetermine the resulting value. In key transport protocols, one party creates or otherwise obtains keying material, and securely transfers it to the other party or parties. Both key agreement and key transport can be achieved using either symmetric or asymmetric techniques. A hybrid key establishment scheme makes use of both symmetric and asymmetric techniques in an attempt to exploit the advantages of both techniques.

V. PROPOSED WORK

Key management services should adhere to the following generic security attributes: Confidentiality. Key management schemes should guarantee key secrecy, that is, ensure the inability of adversaries or unauthorized parties to learn keying material (or even partial keying material).[17] Key authentication. Key authentication is a property whereby a communication entity is assured that only the specifically identified and authenticated communication entity may gain access to the cryptographic key material. Key authentication, in the context of a communication session between two parties, can either be unilateral or mutual: unilateral authentication means that only one party's keying material is authenticated, while mutual authentication involves validating both parties' keying material. Possession of the key is in fact independent of key authentication. Key authentication, without knowledge that the intended recipient actually has the relevant key, is referred to as implicit key authentication.

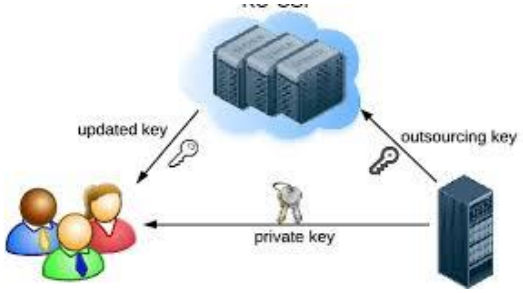

Figure 1

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_____an . It unique solution is X=ai(mod Pi)for 1<=i<=r which is given by X=a1M1X1 + a2M2X2 +_____anMnXn (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) M=m1m2_____mr

Table 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

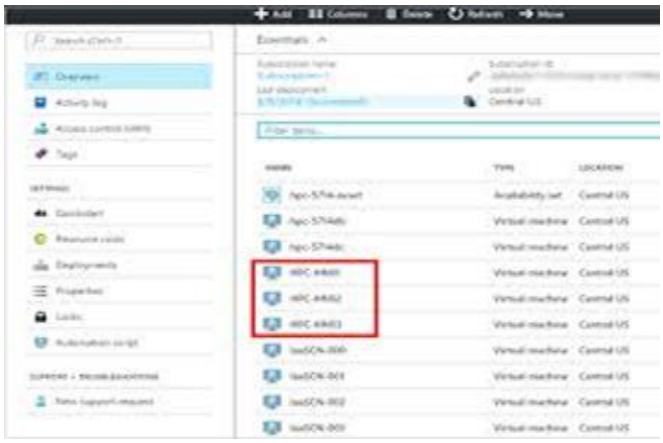

Figure 2

VI. 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 International Journal of Computer Application

VII. CONCLUSION

Key management schemes based on the key pre distribution techniques proposed for sensor networks may be another avenue to solve the key management problem in authority-based MANETs.[19] Another observation is related to the criteria used by researchers to analyze key management schemes for MANETs. Key management schemes are designed either for an —open‖ (self-organized) or —closed‖ (authority-based) network and consequently aimed at different applications. —Open‖ or fully self-organized MANETs have some inherent security implications (such as being vulnerable against the Sybil attack [Douceur 2002]) and must be analyzed accordingly. It is therefore not always possible to compare schemes that assume the existence of a trusted authority with those that are fully self-organized.[21]

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

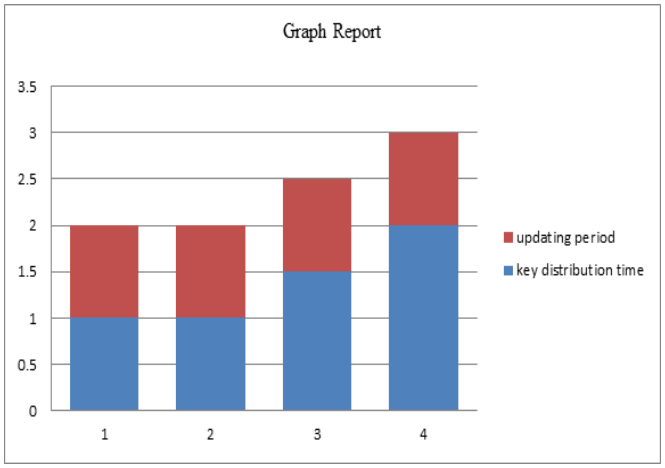

Figure 3

VIII. 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,

[5]. JOHANN VAN DER MERWE, DAWOUD DAWOUD, and STEPHEN McDONALD, Peer-to-Peer Key Management for Mobile Ad Hoc Networks, ACM Computing Surveys, Vol. 39, No. 1,

[6]. ABDUL-RAHMAN, A. AND HAILES, S. 1997. A distributed tust model. In Proceedings of the ACM New Security Paradigms Workshop.

[7]. AKYILDIZ, I. F., SU, W., SANKARASUBRAMANIAM, Y., AND CAYIRCI. 2002. A survey on sensor networks. IEEE Commun. Mag. 40, 8 (Aug.), 102–114. 4ATENIESE, G., STEINER, M., AND TSUDIK, G. 1998. Authenticated group key agreement and friends. In Proceedings of the 5th ACM Conference on Computer and Communications Security.

[8]. AYANOGLU, E., I, C.-L., GITLIN, R. D., AND MAZO, J. E. 1993. Diversity coding for transparent self-healing and fault-tolerant communication networks. IEEE Trans. Commun. 41, 11, 1677–1686.

[9]. BETH, T., MALTE, B., AND BIRGIT, K. 1994. Valuation of trust in open networks. In Proceedings of the Third European Symposium on Research in Computer Security. 7BLOM, R. 1985. An optimal class of symmetric key generation systems. In Proceedings of EUROCRYPT'84.

[10]. BOBBA, R. B., ESCHENAUER, L., GLIGOR, V. D., AND ARBAUGH, W. 2003. Bootstrapping security associations for routing in mobile ad-hoc networks. In Proceedings of the IEEE Global Telecommunications Conference.

[11]. BONEH, D. AND FRANKLIN, M. 2001. Identity-based encryption from weil pairing. In Proceedings of the Conference on Advances in Cryptology (CRYPTO'01).

[12]. BROCH, J. AND JOHNSON, D. B. 1999. The dynamic source routing protocol for mobile ad hoc networks. IETF Internet Draft. October.

[13]. BUNDO, C., DE SANTIS, A., HERZBERG, A., KUTTEN, S., VACCARO, U., AND YUNG, M. 1993. Perfectly-secure key distribution for dynamic conferences. In Proceedings of CRYPTO'92.

[14]. BUTTYAN, L. 2001. Building blocks for secure services: Authenticated key transport and rational exchange protocols. Ph.D. dissertation. Universite Technique de Budapest, Budapest, Hungary.

[15]. BUTTYAN, L. AND HUBAUX, J. P. 2003. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM Mobile Netw. Appl. 8, 5, 579–592.

[16]. CAGALJ, M., CAPKUN, S., AND HUBAUX, J. 2006. Key agreement in peer-to-peer wireless networks. Proc. IEEE (Special Issue on Cryptography and Security) 94, 2, 467–478. 17CAPKUN, S., BUTTYAN, L., ANDHUBAUX, J.-P. 2003a. Mobility helps security in ad hoc networks. In Proceedings of MobiHoc.

[17]. CAPKUN, S., BUTTYAN, L., AND HUBAUX, J.-P. 2003b. Self-organized public-key management for mobile ad hoc networks. IEEE Trans. Mobile Comput. 2, 1, 52–64.

[18]. CAPKUN, S., HUBAUX, J., AND BUTTYAN, L. 2006. Mobility helps peer-to-peer security. IEEE Trans. Mobile Comput. 5, 1, 43–51.

[19]. CARTER, C., YI, S., RATANCHANDANI, P., AND KRAVETS, R. 2003. Manycast: Exploring the space between anycast and multicast in ad hoc networks. In Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MOBICOM'03).

[20]. CHA, J. C. AND CHEON, J. H. 2003. An identity-based signature from gap diffie-hellman groups. In Proceedings of the Conference on Public Key Cryptography (PKI'03).

[21]. 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.

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

[23]. 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.

[24]. 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.

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