An Energy Efficient Integrated Framework For Secure Routing And Key Management In Mobile Ad-Hoc Networks

Renu, Sanjeev Sharma

Abstract - (MANETs) are being very trendy these days and used in a number of applications where security is challange like military operations or other sensitive projects, whereby if the network is compromised then the outcomes can be terrible. It would not be easy task to apply energy efficient and reliable routing in MANETs, because it will not be possible to recharge / replace a battery of mobile node. To take full benefit of the lifetime of nodes, traffic should be routed in a way that energy usage also should be minimized. A lot of security proposal have came which address different protocol stack but no scheme is fully integrated with respect of energy and security. The proposed integrated approach based on Identity cryptography which belongs to the class of pair wise cryptography, addresses all the concerns like secure routing and key management as well as energy.It is a general method for providing routing security and can be applied to any routing protocols.

Keywords: Cryptography, MANET, communication, routing

1. INTRODUCTION

Security during routing becomes very important in sensitive application .Designing of a routing protocol that can ensure the security and efficient quality of service in general is a great challenge .Various proposals for securing the process of routing in MANETs came into account but none of them includes the dependency cycle. Although cryptographic techniques have been widely used in routing to shield routing information from adversary, such an approach may not be practical for real MANETs due to deep computational overhead and lack of capability of spotting attacking nodes given the high mobility of MANETs where nodes can join or leave the networks [1].Energy management is a genuine issue at communication time and idle time in most of the applications of MANETs such as WSN,UAANETand IoT etc.In the proposed ID based scheme the sender can use the receiver's identity of public key to encrypt message, and the receiver can decrypt the cipher text by his own private key obtained from the public key generation according to his identity.The paper also consider the energy efficiency factor by reducing the power consumed in communication as well as in computation.

The whole paper is arranged as: Section 2 presents related work in key management for secure routing in MANETs.Section 3 explains the motivation behind the work,Section 4 describes the proposed identity based security method including various phases and Section 5 is kept for Performance evaluation with basic security services.Last section concludes the work with future aspects in this area.

2. LITERATURE SURVEY

various mechanisms and protocols have been proposed for preserving energy and securing MANETs, but no solutions can directly be applied for this environment. In general, a routing protocol which does not require large tables to be downloaded or greater number of calculations is preferable, the amount of data compression before transmission decreases the power consumed for communication although the number of computation tasks increases.Power-aware Multiple Access Protocol PAMAS [4] uses model to make the use of nodes running low on battery power by making the nodes off when they are not in use. Other power-aware routing protocol [5] Online Max-Min (OMM) by Li et al given by maximizing the minimal residual power, to reduce the rate of overloaded nodes. . Basic cryptographyworks with Public Key Infrastructure (PKI)and suffers with the security of a central control Authority (CA) for issuing digital certificates .PKI also have overhead storage of public key certificates. In 1984, Shamir [9] suggested the solution as identity-based cryptography to avoid these situation .Boneh etc proposed the first model of ID based security scheme based on bilinear maps on an elliptic curve.Previous proposed methods are not suitable for mobile networks lacking with centralized key management agent because they assumed that all nodes in the network are helpful and truthful during the routing process. Constrained devices with battery power, storage capacity and processing capacity are not compatible withtraditional cryptographic algorithms those are executed with high processing, storage and power consumption.

3. MOTIVATION

As we found from previous papers,all routing messages have two type of fields one is static and can not be changed ,another is modifiable by intermediate nodes. No one has differentiate these static fields and changeable fields . The receiver not be able to detect misbehavior because no history is available . Digital signature can work as authentication mechanism to ensure that the changeable fields are not illegally modified. Digital signatures from all to the intermediate node are appended and verified by the next hope

Revised Manuscript Received on December 22, 2018.

Renu, Rajiv Gandhi Technological University, Bhopal, India (e-mail: renutrivedi@rediffmail.com)

Sanjeev Sharma, Rajiv Gandhi Technological University, Bhopal, India

to check the misbehavior.Traditional methods for creating digital signature are very complex and can not be implemented in MAANET due to thehigh computation overhead.In this paper ID-based short signature scheme is proposed which can be add-up as security extension of AODV,LEACH, DSR or other routing protocols without any burden of management of revocation list of certificate[13].

4. PROPOSED WORK AND RESULTS

So many proposals came for securing the routing in MANETs. They all used cryptographic techniques to protect routing information, these are not practical for MANETs due to heavy overhead and lack of capability of spotting attackers.No one suggested the the solution which can directely be implemented in MANET.Secure routing will work with encryption and authentication of each message at each intermediate node to avoid attacks during routing for that keys should be available before routing and it will only be possible if both are independent.Key management must be available before secure routing to break the inter dependency cycle.To start the overall working we considered secure broadcasting to initiate Secure routing.The security of broadcasting can be implemented by utilizing advantages of public cryptography.The paper presented combined solution for secure routing and key management with identity based cryptography.

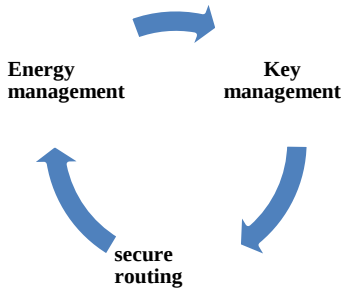

Fig. 1: Schema of Integrated Security Framework

4.1 How it works as a whole:

The framework comprises of three modules ie.Energy management, Key management and secures routing

4.1.1 Energy Preserving:

Energy management is important because here networks have been developed to provide communication for an environment where no fixed infrastructure exists. In adhoc netwok power consumption is mainly due to transmission and reception of bits. Whenever a node remains active, it consumes power. Even when it is not active, but is in the listening mode waiting for the packets, the battery keeps discharging. The computation power consumption refers to the power spent in calculations that take place in the nodes for routing and other decisions. A energy efficient routing protocol avoids to download huge tables and limited calculations is preferred.As we know that, nodes heve very limited battery power so we need a balanceed approach must be developed for security computation and lifetime of the node.Hard security protocols are not easy to implement and light security protocols can be easily attacked.

4.1.2 Key management:

It is the hert of any cryptosystem.Key management is a dealing with the generationof key,storage, managemnt and re-genration of keys. Successful key management is a major challange to the security of a network. We gave the solution for KM-SR interdependency cycle problem using identity based cryptography.The scheme works for confidentiality, integrity, authentication in energy efficient way.Various Choices of key management came in the existance as Trustworthy server scheme in which process of establishing the key agreement between two nodes is executed in the centralized server. Each node has given a single secret key. This is energy expensive due to transmission overhead.Other schemes are based on Self configuration with the help of public key cryptography as RSA and DH which suffers with complex computations.The method based on Key-predistribution is energy efficient bacause it does not bring extra overhead for key exchange.So for making our approach energy efficient we chosen the last scheme based on ID based cryptography

4.1.3 Secure routing:

Secure routing plays vital role when transferring sensitive information between two nodes[13]. For that security mechanism is required to handle different type of existing attacks . ID based approach leads to reduce impersonating, packet dropping and routing attacks by utilizing the combination of ID and transmission time.

4.2 Identity-based cryptography :

In IBC a public string is used as a public key. The scheme is suitable for MANET because it does not require any infrastructure.It works without certificate distribution, and without any interaction between nodes.

The public key can be inherited from email address, IP address etc. The schemes allow a node to create a public key from a ID. Private key generator (PKG), is used to generate private keys to all the nodes in the network.for that PKG launches a master public key, and keeps the corresponding master private key . A party can get a public key by merging master public key with the ID.

In this paper, integrated framework has been proposed to break the cycle of dependency between secure routing and security services.The method utilize pool of keys and pairing-based key generation techniques to break cycle. A. Shamir's [8] secret sharing technique, is utilized for distributing the load of PKG among all nodes, with some slight modifications .This methods also took the best feature of threshold cryptography for shared secret and private key generation so that single point of failure can be removed It distribute cryptographic services to all the network nodes.This brings a minimum overhead on the network by using Shamir's [8] secret sharing technique.

4.3 Steps in key management proposed method

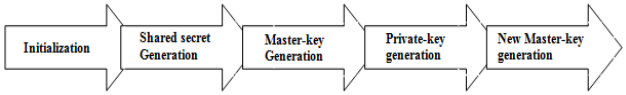

Fig. 1. Steps of proposed method

4.3.1. First Phase as Initialization:

Here p and q are two large primes and E is an elliptic curve of the form y2 = x3+ ax +b over the finite field Fp..G1 and G2 are be a q order subgroups over the curve and group of the finite field respectively.Here It is assumed that the discrete logarithm problem not so easy to cover The proposed IBC system deploys the bilinear mapping that is bilinear, nondegenerative and Computable. Variation on bilinear maps are available such as bilinear Diffie–Hellman acts as :

If k ,Z are input, generates a prime number (q); G1 and G2 (of order q)

2. calculate the hash function H :{0,1} →G .

3. Find P =generator of G1.

4. Generated parameters P, G1 ,G2,q,e,H are public and send to all at the beginning.

4.3.2. Shared Key Generation:

Now the challenge is to develop a shared key for secure communications between nodes.Various popular Key generation algorithms exists like Diffie hellmen,RSA Elgamal. By using diffie hellmen we generates a shared key based on public system parameters.The shared key discovery phase begins after deployment of the nodes. Each node broadcasts its key identifiers without any form of encryption. The nodes that are in radio range of each other discover the shared keys by comparison. However, it is possible that nodes discover shared keys privately by hiding their key sharing pattern.

4.3.3. Distributed Master-Key Generation:

The applied mechanism does not rely on a centralized third party to get master key because of the constrained environment of MANET so we divide a master key into shares, and distribute the shares. This key can be retrieved back in a distributed manner [8], the proposed method utilizes Shamir's secret-sharing method [9] without a trusted authority.

4.3.4. Generation of Private-Key:

The method has recursive key update phases where each phase is identified with a it's ID. In the initialization phase, a random seed, salt1, is preloaded to Every node has a random value as a seed and this phase ID. Each pair has both node specific and phase-specific information . T ID and so as to bind To identity a node ,MAC and Id is used as combined

5. PERFORMANCE EVALUATION

The security performance of any network depend on its cryptography system. Our proposed method is analyzed in this section to show that it can achieve important security services with a manageable cost.

5.1. Computational efficiency:

Proposed identity-based cryptography schemes is said computationally efficient, because of bilinear non degenerate maps and pairing of elements from one cyclic group to other.Efficiency of proposed scheme is based on bilinear maps as one-way functions.It means that bit is easy to compute their result given a pair of operands but difficult in reverse.An intruder cannot determine the private key of an un compromised device. The proposed method can be called as resilient against capturing the device.

5.2 Confidentiality:

confidentiality of key shares is guaranteed through the pool method. First nodes shares identifiers and may use puzzles.After the shared-key discovery phase, Then nodes share mutual common info to implement the security of the messages. In Identity based system we use secure links.Private share are encrypted by the IBC system.Confidentiality is assured of transmitted data in IBC system.

5.3 Integrity:

In the proposed system, all messages got encrypted by the public key of the recieving node and signed with private key of the sending node.So,confirmation of the integrity of message is achieved..

5.4 Authentication:

Generating group key with the help of ID based cryptographic technique.assures forauthentication In the proposed method all messages are signed by a digital signature of sender.An attacher cannot create valid signature for a altered message which is enough to assure the authentication of messages

5.5 Energy:

Energy of a node is indicator for the strength and life required for survival in the network . Energy consumption is defined as the communication overhead of the nodes where a certain number of false data are injected in to a network. In recent years, various energy efficient routing protocols have been proposed. The proposed scheme has unique characteristics and utilizes different preserving mechanisms on energy consumption.The scheme works for preserving energy by reducing the power consumed in communication as well as in computation.

5.6 Throughput:

Quantity of data that can be sent from the sender to the reciever, determines the throughput .Identity-based security method is based on the particular bilinear maps and one-way functions which increases the throughput.

6. CONCLUSION

For authentication process, the interaction occurs so many times in previous traditional methods which increases the load over the network and will suffer badly when the MANET will be scaled up.The paper presented an ID Based mutual Authentication solution for secure routing and key management in energy preserving way by reducing the no of massage exchanged and no of keys required . This method

divides the key among participating node of MANET and utilize group secret key to proceed further.The work provides safety of data confidentiality before working of system, without authorization.Some technique will be identified to solve this problem in future.Over all we noticed that any cryptosystem need to be executed with high processing, storage and power consumption and can not be directly implemented in real MANETs. For all of the above reason trust based security solution is being popular area in the research of security of constrained networks.

REFERENCES

1. L Junhai, X Liu, Y Danxia, Research on Mul-ticast Routing Protocols for Mobile Ad-Hoc Net-worksComputer Networks – Elsevier, 2008.
2. Kapil, A, etc "Identity-Based Key Manage-ment in MANETs using Public Key Cryptog-raphy."International Journal of Security (IJS) 3.1(2009): 1-26
3. V. N. Talooki, H. Marques, and J. Rodriguez, \Energy efficient dynamic manet on-demand routing protocol," Symposium and Workshops on a World of Wireless, Mobile and Multimedia Net-works 2013.
4. M. Maleki, K. Dantu and M. Pedram, Power-Aware On-Demand Routing Protocols for Mobile AdHoc Networks, International Symposium on Low Power Electronics and Design,pp. 72-75, 2002.
5. Q. Li, J. Aslam, D. Rus, Online Power Aware Routing, Proceedings of International Conference on Mobile Computing and Networking (Mo-biCom'2001), 2001.
6. I. Stojmenovic and X. Lin, Power Aware Lo-calized Routing in Wireless Networks, IEEE Transactions on Parallel and Distributed Systems, vol. 12, no. 11, pp. 1122-1133, November 2001.
7. R. A. Shaikh, S. Lee, M. A. U. Khan, and Y. J. Song, "LSec:lightweight security protocol for distributed wireless sensor net-work", Lecture Notes in Computer Science, vol. 4217, 2006.
8. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in Advances in Cryptology, Berlin, Germany: Springer Berlin Heidelberg, 1985, pp. 47–53.
9. A. Shamir, "How to Share a Secret," Commun. ACM, vol. 22, no.11, Nov. 1979, pp. 612–613
10. B. Lee et al., "Secure Key Issuing in ID-Based Cryptography," inProc. Workshop Aus-tralasian Inf. Security, Data Mining WebIntell., Softw. Int., vol. 32, Australia: Australian Com-puter SocietyInc., 2004,
11. B. A. Mahmood and D. Manivannan, \Position based and hybrid routing protocols for mobile ad hoc networks: a survey," Wireless Per-sonal Communications,vol. 832015.
12. Renu M.,Dr. Sanjeev S.,Inderpreet K."Secret Sharing for Key Management Scheme in Ad-hoc Networks" Proc. IEEE International Conference on advanced computing & communication tech-nologies
13. Y. Ren et al., "Identity-Based Key Issuing Protocol for Ad Hoc Networks," IEEE Int. Conf. Comput. Intell. Security, Harbin,China, Dec. 15–19, 2007, pp. 917–921.
14. Renu Mishra, Inderpreet Kaur & Sanjeev Sharma" New Trust based security method for mobile ad-hoc networks" International Journal of Computer Science and Security (IJCSS), Volume (4), Issue: (3) 346 -3512 June -July010
15. H. Deng and D.P. Agrawal, "TIDS: Thresh-old and Identity-Based Security Scheme for Wireless Ad Hoc Networks," Ad Hoc Netw.,vol. 2, no. 3, July 2004, pp. 291–307.
16. Sandeep Saxena, Goutam Sanyal and Shashank Srivastava"Mutual Authentication Pro-tocol Using IdentityBased Shared Secret Key in Cloud Environments"IEEE International Confer-ence (ICRAIE-2014),