iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VII **Month of publication:** July 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Asymmetric Key management in Wireless Ad-hoc network- A Survey

Rajneesh Kumar [1] KKS Gautam[2]

[1] *Assistant Professor, Maitery College, University of Delhi,*
[2]*Assistant Professor, Rajdhani College, University of Delhi*

Abstract: As Mobile Ad-hoc network(MANET) has no fixed infrastructure, due to which securing MANET is always a major challenge. All efficient cryptosystem require a Key management. In fact, for a good cryptosystem require an effective key management. In mobile ad hoc networks, the computational load and complexity for keymanagement are mainly related to availably of node's resources and the dynamicnature of network topology. In this study we are trying to identify various methods for effective asymmetric key management in MANET.

1. INTRODUCTION

Although,high speed data is possible in mobiletechnology because of 3G/4G.But people prefer Bluetooth and WiFi more than 3G due to easiness and quickness. Because of this, there is significant growth of mobile computing devices, which mainly include laptops, smart phone and other handheld digital devices. It has encouraged a revolutionary change in the computing world, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [3]. The Mobile Ad Hoc Network is one of them research. Whenever, we talk about communication and information transfer, the security is major concern. The key management is involved in all effective secure communication. This paper has organized as follows. in second section the general introduction of security in ad-hoc network; followed by key management in third section and in forth section, various asymmetric algorithms are briefly discussed . In last section, we end with conclusion and future directions.

2. AD-HOC NETWORK AND SECURITY

A Ad hoc network is a collection of wireless mobile hosts that form a temporary network without the aid of any centralized server or support. Every mobile node operates as a host as well as a router, forwarding packets for other mobile nodes in the network that may be multiple hops away from each other. The applications of MANETs can be worked when bad weather, earthquake or weak mobile network.

In order to transmit packets in MANET from one node to other, they should be in range. Otherwise direct transmission is not possible. As in MANET the mobile node can act as router hence intermediate node between source and destination forward packets toward the other node in range. However the real Ad-hoc network has no proper network structure therefore it is very hard to find fix path. Therefore, proper routing algorithm is needed that can successfully packets from sender to proper destination.

Mobile ad hoc networks have far more vulnerabilities than the traditional wired networks. Security is more difficult to maintain in the mobile ad hoc network than in the wired network. Different problems, such as Lack of Secure Boundaries, Threats from Compromised nodes Inside the Network, Lack of Centralized Management Facility, and restricted Power Supply are identified.

Security Issues in Ad-Hoc networks

Layer	Security Issues
Application	Detecting and preventing virus , worms and other malicious program
Transport	Authenticating and securing end to end communication
Network	Protecting ad-hoc routing and forwarding protocols
Link	Protecting wireless MAC protocol and providing link layer security
Physical	Protecting signal jamming and denial of service attack

3. KEY MANAGEMENT

Key management is a basic part of efficient secure communication. Key distribution center play major role to distribute key between sender and receiverthrough insecure channels. There are mainly two different type of key distribution:- centralize and distributed. The frameworks are based on a centralized trusted third party (TTP). For example, a certificate authority (CA) is the TTP in public key infrastructure (PKI), a key distribution center (KDC) is the TTP in the symmetric system, whilein PGP no such a trusted entity is asside and is encrypted by the public-key algorithm. Then it is delivered and recovered at the otherend. In the Diffie-Hellman (DH) scheme [4], the communication parties at both sides exchangesome public information and generate a session key on both ends. Several enhanced DH schemeshave been invented to counter man-in-the-middle attacks. In addition, a multi-way challengeresponse protocol, such as Needham-Schroeder [5], can also be used. Kerberos [5], which isbased on a variant of Needham-Schroeder, is an authentication protocol used in many realsystems, including Microsoft Windows. However, in MANETs, the lack of a central controlfacility, the limited computing resources, dynamic network topology, and the difficulty ofnetwork synchronization all contribute to the complexity of key management protocols.

Key integrity and ownership should be protected from advanced key attacks. Digital signatures,hash functions, and the hash function based message authentication code (HMAC) [12] aretechniques used for data authentication and/or integrity purposes. Similarly, the public key isprotected by the public-key certificate, in which a trusted entity called the certification authority(CA) in PKI vouches for the binding of the public key with the owner's identity. In systemslacking a TTP, the public-key certificate is vouched for by peer nodes in a distributed manner,such as pretty good privacy (PGP) [4]. In some distributed approaches, the system secret isdistributed to a subset or all of the network hosts based on threshold cryptography. Obviously, acertificate cannot prove whether an entity is "good" or "bad". However, it can prove ownershipof a key. Certificates are mainly used for key authentication.

A cryptographic key could be compromised or disclosed after a certain period of usage. Since thekey should no longer be usable after its disclosure, some mechanism is required to enforce thisrule. In PKI, this can be done implicitly or explicitly. The certificate contains the lifetime ofvalidity - it is not useful after expiration. However, in some cases, the private key could bedisclosed during the valid period, in which case the CA needs to revoke a certificate explicitlyand notify the network by posting it onto the certificate revocation list (CRL) to prevent itsusage.

Key management for large dynamic groups is a difficult problem because of scalability andsecurity. Each time a new member is added or an old member is evicted from the group, thegroup key must be changed to ensure backward and forward security. Backward security meansthat new members cannot determine any past group key and discover the previous groupcommunication messages. Forward security means that evicted members cannot determine anyfuture group key and discover the subsequent group communication information. The group keymanagement should also be able to resist against colluded members.

Therecan be three possible trust model: (1) centralizemodel[2][10][12] in which a fixed centralize certificate authority is available. (2) Decentralize model[3] where trust model is present in every system which is not

possible. To implement right distributed system the public key is distributed in entire network, while private key is divided in sub-key and distributed to group of systems. (3) Hybrid model[8] is combination of both models. It takes advantage of the positive aspects of two different trust systems..

4. ASYMMETRIC KEY MANAGEMENT

There are two type of key: symmetric and asymmetric key.Symmetric key, where encrypting and decrypting are similar .And asymmetric key, where encrypting and decrypting key are different from each other. In this section we are discussing asymmetric key management scheme only.

4.1 Secure Routing Protocol (SRP)

SRP is a decentralized public key management protocol [3][18][19][7]. In the system, there are n servers, which are responsible for public-key certificate services. Therefore, the system can tolerate t-1 compromised servers. Servers can proactively refresh the secret shares using the proactive secret sharing (PSS) [11] techniques or by adjusting the configuration structure based on share redistribution techniques to handle compromised servers or system failure. The new shares are not dependent of the old ones; therefore mobile attackers would have to compromise a threshold number of servers in a very short amount of time.Therefore, the success of adversaries will be decreased.

4.1 Ubiquitous and Robust Access Control (URSA)

URSA is a localized key management scheme [6] [14] URSA protocol whichis also based on threshold cryptography as in SRP [3]. There is difference between URSA and SRP, in URSA, all nodes are servers and are capable of producing a partialcertificate, while in SRP only server nodes can produce certificates. Thus, certificate services aredistributed to all nodes in the network. URSA also proposed a distributed self-initialization phasethat allows a newly joined node to obtain secret shares by contacting a coalition of k neighboringnodes without requiring the existence of an online secret share dealer. The basic idea is to extendthe PSS technique by shuffling the partial shares instead of shuffling the secret sharingpolynomials. The purpose of this shuffling process is to prevent deducing the original secretshare from a resulting share.

4.2 Mobile Certificate Authority (MOCA)

MOCA[13] is a decentralized key management scheme where acertificate service is distributed to Mobile Certificate Authority (MOCA) nodes. MOCA nodesare chosen based on heterogeneity if the nodes are physically more secure and computationallymore powerful. In cases where nodes are equally equipped, they are selected randomly from thenetwork. The trust model of this scheme is a decentralized model since the functionality of CA isdistributed to a subset of nodes. A service-requesting node can locate $k + \alpha$ MOCA node eitherrandomly, based on the shortest path, or according to the freshest path in its route cache.However, the critical question is how nodes can discover those paths securely since most secure routing protocols are based on the establishment of a key service in advance.

4.3 Composite Key Management

A composite key management[8] is a combination of the centralized trust and the fully distributed certificate chaining trust models. In this scheme, the positive aspects of two different trust systems are included. The basic idea is to incorporate a TTP into the certificate graph. Here, the TTP is a virtual CA node that represents all nodes that comprise the virtual CA. Some authentication metrics, such as confidence value, are introduced in order to “glue” two trusted systems. A node certified by a CA is trusted with a higher confidence level.

4.4 Self-organized Key Management

A fully distributed key management scheme given in[5] based on the web-of-trust model that is similar to PGP [4]. The basic idea is that each user acts asits own authority and issues public key certificates to other users. A user needs to maintain twolocal certificate repositories. One is called the non-updated certificate repository and the otherone is called the updated certificate repository. The reason a node maintains a non-updatedcertificate repository is to provide a better estimate of the certificate graph.

Key authentication isperformed via chains of public key certificates that are obtained from other nodes throughcertificate exchanging, and are stored in local repositories.

4.5 Secure and efficient key management (SEKM) scheme

A secure and efficient key management (SEKM) [15][16][17] scheme is designed to provide efficient share updating among servers and to quickly respond to certificate updating, which are two major challenges in a distributed CA scheme. The basic idea is that server nodes form an underlying service group for efficient communication. For efficiency, only a subset of the server nodes initiates the share update phase in each round. A ticket-based scheme is introduced for efficient certificate updating. Normally, because of share updating, recently joining servers could be isolated from the system if they carry outdated certificates. SEKM creates a view of CA and provides secure and efficient certificate service in the mobile and ad hoc environment.

5. CONCLUSION AND FUTURE DIRECTIONS

In this study we have identify various asymmetric key management in MANET. These techniques either centralize or decentralize approach. It is found that centralize approach is simple but it key management depends on central node. While decentralize is robust but it is complex. After improving both algorithms can provide effective security.

The dynamic conferencing or multicasting in MANETs, is becoming an popular research area. Most of researchers, are trying to solve key or group keys for dynamic session only. The security of group communication involves the management of group keys. The tree-based structures are utilized effectively when a central or virtual central control entity is available. Most contributory group key distributions are based on DH protocol with different implementations.

REFERENCES

[1] Zhou, L. and Haas, Z. (1999). Securing Ad Hoc Networks, IEEE Network Magazine vol.13, no. 6, pp. 24-30.

[2] Wu, B., Chen, J., Wu, J., and Cardei, M. (2006). A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. Wireless/Mobile Network Security, Springer. Chapter 12.

[3] Saloma, A. (1996). Public-Key Cryptography, Springer-Verlag.

[4] Burnett, S. and Paine, S. (2001). RSA Security's Official Guide to Cryptography, RSA Press.

[5] Tanenbaum, A. (2002). Network Security, Chapter 8, Computer Networks. Prentice Hall PTR, 4th Edition.

[6] Stallings, W. (2002). Wireless Communication and Networks, Pearson Education.

[7]Stadler, M. (1996).Publicly Verifiable Secret Sharing.Proceeding of Eurocrypt'96. pp. 190-199.

[8] Yi, S. and Kravets, R. (2004). Composite Key Management for Ad Hoc Networks. Proc. of the 1stAnnual International Conference on Mobile and Ubiquitous Systems: Networking and Services(MobiQuitous'04), pp. 52-61.

[9] Nichols, R. and Lekkas, P. (2002). Wireless Security-Models, Threats, and Solutions, McGraw ill,Chapter 7.

[10] Kaufman, C., Perlman, R., and Speciner, M. (2002). Network Security Private Communication in aPublic World, Prentice Hall PTR.

[11] Herzberg, A., Jarecki, S., Krawczyk, H., and Yung, H. (1995). Proactive Secret Sharing or: How toCope With Perpetual Leakage. Proceedings of Crypto'95, vol. 5, pp. 339–52.

[12]Menezes, A., Oorschot, P., and Vanstone, S. (1996). Handbook of Applied Cryptography, CRCPress.

[13] Yi, S., Naldurg, P., and Kravets, R. (2002). Security Aware Ad Hoc Routing for Wireless Networks. Report No.UIUCDCS-R-2002-2290, UIUC.

[14]Luo, H., Zerfos, P., Kong, J., Lu, S., and Zhang, L. (2001). Providing Robust and UbiquitousSecurity Support for Mobile Ad-hoc Networks.Proceeding of The 9th International Conference onNetwork Protocols.

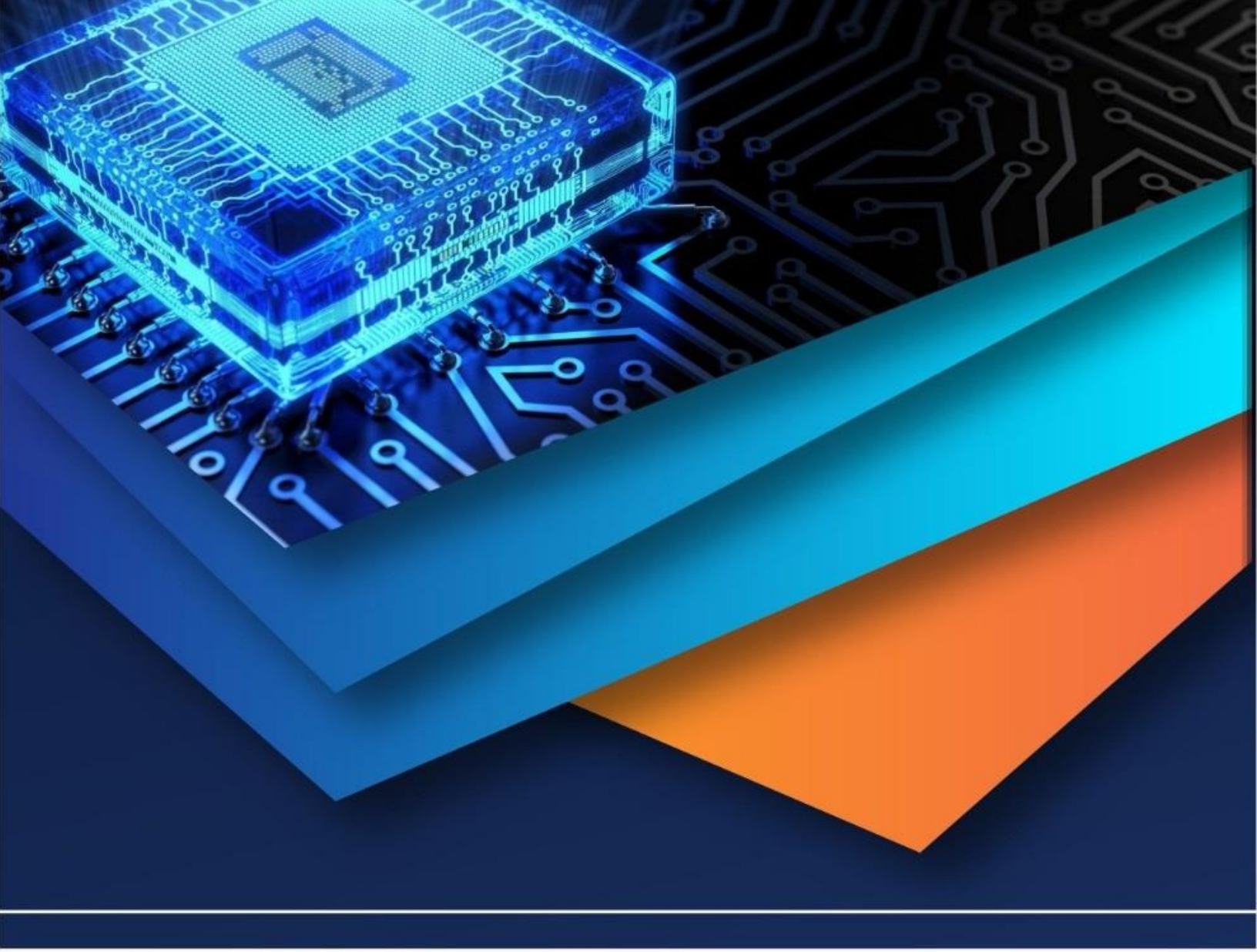
[15] Wu, B., Wu, J., Fernandez, E., Magliveras, S., and Ilyas, M. (2005). Secure and Efficient KeyManagement in Mobile Ad Hoc Networks.Proc. of 19th IEEE International Parallel & DistributedProcessing Symposium, Denver.

[16] Wu, B., Wu, J., Fernandez, E., Ilyas, M., and Magliveras, S. (2005). Secure and Efficient KeyManagement Scheme in Mobile Ad Hoc Networks.Journal of Network and Computer Applications(JCNA).

[17] Bing Wu, Jie Wu, at el. "Secure and efficient key management in mobile ad hoc networks", Journal of Network and Computer Applications. ELSEVIER, 2005

[18] Shamir, A. (1979). How to Share a Secret. Communications ACM 1979; 22(11), pp. 612–613.

[19] Wong, T., Wang, C., and Wing, J. (2002). Verifiable Secret Redistribution for Threshold Sharing Schemes. Technical Report, CMU-CS-02-114-R, School of Computer Science, Carnegie Mellon University.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY