International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017(O)
Issue 1, Volume 2 (January 2015) ISSN: 2349-7009(P)
www.ijiris.com

Towards the security issues in Mobile Ad Hoc Networks

Shabnam Kasra-Kermanshahi*
Faculty of Computing, Universiti Teknologi Malaysia

Mazleena Salleh
Faculty of Computing, Universiti Teknologi Malaysia

Abstract— Mobile Ad hoc Networks (MANETs) are wireless networks consisted of mobile free nodes that can move anywhere at any time without the need to any fixed infrastructure or any centralized administration. In this category of networks existing nodes must rely on each other to play the role of routers or switches instead of using central ones. The self-organized nature of such environments made MANETs vulnerable against many security threats. As a result, providing security requirements in MANETs is one of the most interesting challenges in such a network. In this group of networks, the use of cryptographic solutions is one of the most interesting security issues. The importance of this scientific area in MANETs is more drastic by considering that mentioned schemes must be lightweight enough to be appropriate for resource constrained platforms in such environment. This paper has tried to represent the position of cryptographic issues in MANETs. Moreover, security issues in mobile Ad hoc networks beside of different classes of public key cryptosystems have been introduced.

Keywords— MANETs, Security issues, Identity Based cryptography, Certificateless cryptography

I. INTRODUCTION

These days, popularity of collaborative and mobile applications in wireless networks especially in MANETs led to making them suitable for many security sensitive applications (e.g. military ones). However, due to the especial features of this category of networks, providing security in such environments is one of the significant challenging issues. Early suggested solutions were mostly based on the attack-oriented approaches. More precisely, they have tried to detect or prevent some sorts of attacks [1-10]. Afterward, Cryptography has been used to provide a general design framework [11]. In fact, the nature of resource constrained nodes is one of the significant problems that enforced the developers to propose lightweight and less resource consuming cryptographic secure schemes in MANETs.

Mentioned reasons above were sufficient to persuade many researchers to emphasize on lightweight cryptographic schemes in order to support a large variety of security requirements in mobile ad hoc networks. To reach this goal, traditional public key cryptosystems such as RSA or DSA seem to be not acceptable to use in such networks. This viewpoint was the fundamental concept of many cryptographic schemes that relied on symmetric cryptosystems[12]. For instance, it is possible to refer to the use of symmetric cryptographic schemes such as RC5 [13] and Skip-Jack [14] in resource constrained platforms for many years [15]. However, symmetric cryptosystems suffer from many problems such as not providing non-repudiation services and complex key-management problem in compare with public key ones.

The advantages of using public key cryptosystems (e.g. easier key management security services and less overhead of transmitting processes [16, 17]) caused that many researchers have tried to propose practical public key cryptographic schemes for mentioned resource constrained environments. Obviously, one of the most important general issues regarding to the use of public key cryptographic schemes (not only in mobile nodes) is to ensure entities about the validity of the public key of other authorized ones. The use of Certification Authorities in the context of Public Key Infrastructure is one of the prevalent solutions to reach this goal. However, the cost of managing and implementing mentioned Certification Authorities seems to make this solution impractical in mobile ad hoc networks. The main factor of this drawback in such an environment is the need to expensive processes such as storing, exchanging and verifying the certificates [15].

In order to solve mentioned problem, Adi Shamir propounded the idea of Identity-based cryptography in 1984 [18]. After that, this idea remained an open problem for seventeen years, until Boneh and Franklin in [19] could represent some solutions to make this idea practical. The main idea of Identity-based cryptosystems is the use of entities' uniquely identified identifier such as email address, social security number, network IP address, etc. as their public key. Therefore, the use of this method guarantees that any public key of existing entities is always valid from other entities' perspective. As a result, entities do not need any certificate for utilized public-keys.

One of the significant attributes of this category of public key cryptosystems is that existing entities must utilize a special-purpose third party called PKG for extracting their private key. This nature of Identity-based cryptosystems in turn leads to another drawback named Key Escrow problem. To overcome this problem, pioneered by Al-Riyami and Paterson [20] many researchers have tried to propose another category of public key cryptosystems named Certificateless PKC. Based on this perspective, many Certificateless public key cryptosystems have been proposed in the context of mobile ad hoc networks [21, 22].

II. MOBILE AD HOC NETWORK

The purpose of this section is to introduce the mobile ad hoc networks comprehensively. This section consists of two main subsections. The first subsection assigns to the history of MANETs, while the second one investigates the characteristics of these networks.

© 2015, IJIRIS- All Rights Reserved

A. History of Mobile Ad hoc Network

The history of mobile ad hoc networks came back to Packet Radio Networking project in 1972 that was done by DARPA .In this project all network devices were mobile but with very limited movements [23, 24]. The Packet Radio Networks had some drawbacks because the utilized devices were prohibitive, big with slow computation capacity and energy consuming. In 1980s, DARPA introduced a new type of mobile technology named "SURAN" that did not suffer from mentioned drawbacks [25]. Afterward, the researchers changed their attitude in the development of MANETs from making the devices smaller and weightless to finding suitable communication approaches for this especial environment. In this way, they proposed multi-hop approach [26, 27] for routing in MANETs instead of broadcasting the packets. The next generation of researches in MANET started from 1990 [28], which focused on its security. Although too many studies were done in this research area, providing security for MANETs is still an open problem. This issue is due to the especial characteristics of MANETs that are explained in the following subsection.

B. Mobile Ad hoc Network characteristics

Mobile Ad hoc Network is an autonomous system of mobile devices that do not relay on any fixed infrastructure (see Fig.1). On one hand, lack of any fixed infrastructure makes these networks suitable for some critical applications such as emergency operations, disaster relief efforts, business indoor applications, civilian outdoor applications, military networks and so on [29, 30]. On the other hand, providing security for MANETs would be one of the most significant challenging issues (more details are provided in the next subsection).

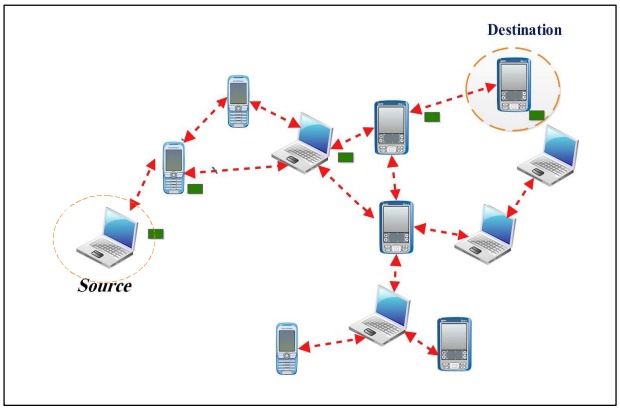

Fig.1 Mobile Ad hoc Network

The characteristics of MANETs can be summarized as followed [29];

(i) Self-configured: Based on this feature, network functions (e.g. routing) must be done by the nodes, to keep the network usable.
(ii) Dynamic topologies: Random movements of the nodes make the topology of the network unpredictable and highly dynamic.
(iii) Resource constrained devices: Nodes are resource constrained in bandwidth, battery, memory, processing capability and computing power.
(iv) Poor physical security: There is a possibility that mobile devices being captured or broken by adversaries.

III. SECURITY ISSUES IN MOBILE AD HOC NETWORKS

Mentioned features above can lead to a set of underlying assumptions and performances and security concerns, which makes the design procedure more challenging. Due to the ability of communication over wireless channels and rapid growth of mobile devices, lack of widely accepted security solutions for this environment, made the research over security of MANETs still an active area [11].

Effective and proven security solutions for traditional networks are not always applicable to MANETs. In fact, attacks (e.g. identity/address spoofing, message tampering/ forgery/ replay) which may be easily detected and prevented in the traditional networks could be very challenging in MANETs. Mentioned issues in mobile ad hoc networks led to the difficulty of achieving security requirements [11].

Similarly to the traditional networks, MANETs need some security requirements which are described below [31]:

(i) Data Confidentiality: keeping data secret from unauthorized entities
(ii) Data Integrity: preventing modification of data by unauthorized entities
(iii) Data Freshness: Keeping data in the correct order and up-to-date
(iv) Data Availability: Ensuring that data will be available on request
(v) Data& Identity Authentication: Verifying that the data or request is coming from a valid sender
(vi) Non-repudiation: Ensuring that a node cannot deny sending a message.

© 2015, IJIRIS- All Rights Reserved

Previously, suggested security solutions by the researchers were mostly based on the attack-oriented approaches that TABLE I illustrates some of them as examples. In fact, after identifying possible threats, they enhanced available schemes or designed a new one. Moreover, proposed schemes based on these approaches just cover limited attacks and could be vulnerable against some other ones or a combination of them [11].

TABLE I. Attack-oriented schemes

Reference	Attack type	Method
[32]	Wormhole[1]	Using packet leash[2] protocol
[33]	Wormhole	SECTOR mechanism
[34]	Blackhole[3]	Security-aware ad hoc routing protocol
[35]	Impersonation and non-repudiation	ARAN[4]
[36]	Modification	Security protocol SEAD

Cryptography has been used to provide a general design framework. Based on the structure of the utilized key, it is possible to categorize cryptosystems in two main groups; symmetric key based and asymmetric key based.

Symmetric key based cryptosystems suffer from some drawbacks regarding to the key management, memory consumption, key refreshment, scalability, and so on that makes them unsuitable for the MANETs [37]. However, there are some schemes that used symmetric cryptography in the context of routing protocols for mobile ad hoc networks [38-40].

Since, asymmetric key based cryptosystems provide more functionality such as authentication and non-repudiation and easier key distribution, they could be a better solution for the MANETs. Due to the importance of this type of cryptosystems, they will be explained in more details in the next section.

A. Public Key cryptosystems

In the public key cryptosystems, each entity possesses a pair of keys; “Public Key” and “Private Key”. As it is obvious from the names of these keys, Public key refers to the key that is known to all communicating entities while the other one must be kept in secret. One of the significant attributes of this category of cryptosystems is that extracting the private key from corresponding public key is very difficult. However, this kind of cryptosystems is not beneficial unless under the condition of supporting trustworthy for the utilized public keys. More precisely, we have to authenticate the public keys and make sure that they belong to the users who are claimed [37].

Public key cryptosystems can be categorized in three main classes, “Traditional public key”, “Identity-based public key”, and “Certificateless public key” which will be discussed in the following sections.

1) Traditional Public key cryptosystems

This type of public key cryptosystems relies on digital certificates provided by a trusted party named Certificate Authority (CA). The main problem of the Traditional PKC is related to the difficulty of complex management of Public Key Infrastructure, which consists of CA, certificate directory, and revocation related entity (for more details refer to [41]).The functionality and drawbacks of the Traditional public key cryptosystems is defined in more details in the following scenarios.

Before sending all cryptographic information on an unsecure channel, the first party must be sure that the obtained second party’s public-key is the correct one. This issue can be investigated in more detail over two steps, which are extracting and verifying the mentioned public key. If we assume that the public-key extraction step is easy and does not need to be focused on, the verifying step would be difficult. However, there is a well-known technique to verify existing public-keys, which is relying on public key certificates provided by CA.

It seems that the use of Digital Signature is a suitable way to rich this goal. This method, in turn imposes some other concerns. First, the used Digital Signature scheme must be cryptographically secure. Second, all existing entities must be able to verify the signature of the other entity who certified the required public-key. By assuming that the utilized Signature scheme cannot be forged, the second concern leads to two other consequences. The first consequence is that the entity who plays the role of a verifier must be sure that the public-key of the signer is valid. Beside of this, the mentioned entity should trust the signer. Clearly, a dishonest signer can replace the second party’s public-key by the public-key of the entity of his choice.

Unfortunately, mentioned two conditions cannot be satisfied easily. To explain the main problem, which is named Certification Path problem, assume that the first entity, Alice, does not know the assigned public-key, which is required to verify the Bob’s certified public-key. In this case, she needs to verify another certificate to obtain the Bob’s public-key.

[1] Packets are gathered from one position in the network and then tunneled to another position.
[2] The attached information to the packet that limit the transmission distance.
[3] An attacker exploits the routing protocol and does not forward packets.
[4] A Secure Routing Protocol for Ad Hoc Networks

© 2015, IJIRIS- All Rights Reserved

Of course, if she is unable to verify the last certificate, this scenario will continue until she can obtain a verifiable certificate. The only solution to the Certification Path problem is assuming that all entities are initially given at least one of the public-keys securely. As a simple solution, one of the mentioned keys can be pre-installed for all existing entities. This simple solution makes all entities able to verify the certificates if there exists a Certification Path to validate the public-keys of existing entities.

An admissible method to implement the solution above is the use of Certification Tree, which can be created by a Certification Authority as a root node, intermediate delegate authorities that are certified by their father node, and finally the last communicating parties as the leaves of the tree. In this method, each entity must possess the public-keys of all intermediate authorities, which are placed between him and the root Certification Authority. As a result, by starting from the shared authority of Alice and Bob, these entities would be able to check the certificate of each other's public-key.

Although it seems that the solution above is perfect, it suffers from the problem of managing the trust to the owner of the first public-key. This problem can be investigated based on two different viewpoints. From a hierarchical organization viewpoint, a trusted system administrator who is responsible to setting up a Certification Authority can solve this problem. Since the administrator is trusted by mentioned organization, other entities can trust him during the communications. Although this solution seems to be perfect for the organizations, from individual party's viewpoint it is not a proper one. The reason is that all parties cannot trust this initial key, which is provided by a company.

To escape the mentioned difficulty above, it is possible to let parties create certificates. Based on this solution, any party can trust a certificate that has been created by a trusted entity as his friend. However, this solution suffers from another significant problem. In the systems based on this solution, individual parties cannot trust an entity which is a friend of their friend (or a friend of one of the friends of their friend and so on) while they never met that entity. As a result, this problem can void the value of certificates in a direct trusted party method. Therefore, this issue can be limited to an expensive and hardly quantifiable method in which last parties could obtain the same key through some independent channels until satisfying by the validity of the considered public-key.

Due to all drawbacks of traditional PKC that mentioned above and the especial nature of the mobile ad hoc networks, the use of these cryptosystems is not popular in this case. However, there are limited number of studies [42-44] that used traditional PKC specifically for this environments.

2) Identity-based Public key cryptosystems

Although Traditional PKC could solve the problem of the validity of authorized entities' Public-key by the use of CA, the need to a valid certificate for CA's public-key in these systems led to a new concern which is Public Key Infrastructure (PKI) complex management. To avoid a large fraction of mentioned problems, Identity-Based cryptography offers a powerful theory. Replacing the users' public-key by their identity (such as telephone number, image, email address, etc.), can lead to eliminate the need to certificates and all consequences of managing them.

The fundamental notification in an Identity-Based cryptosystem is that all involving entities already need to learn some basic information before they communicate with each other. At the very least, they need to obtain the identifier of the other communicating entities. Based on what pointed out by Shamir in [18], the important advantage of Identity-Based cryptosystems is replacing entities' public-key by this identifier.

3) Certificateless public key cryptosystems in MANETs

As mentioned earlier, in an Identity-based cryptosystem each entity must collect its private key from PKG hence PKG can eavesdrop the messages or impersonate entities. This inherent problem in Identity-based cryptosystems called "key escrow". This problem limits the use of Identity-based cryptosystems to closed organizations [45]. Early solutions focus on utilizing more key pairs, using threshold, and considering expiry date for the master key. However, they have some drawbacks that make them unsuitable for MANETs such as too much overhead to the network, more computation /communication for nodes which are resource constrained devices [11].

In 2003, a novel public key cryptosystem was introduced by Al-Riyami and Paterson [20] named "Certificateless public key" that could overcome the key escrow problem while public keys are authenticated without need to the PKI. In this cryptosystem, a trusted third party called Key Generator Center (KGC) is responsible for generating partial private keys for the users. This key is driven by master key (only known by KGC), and the users' identity. Then, each user can produce his private key. The user's private key can be generated by the use of partial private key received from KGC and a secret value chosen by the user hence there is no problem regarding to the key escrow [46]. Since, in the CL-PKC the partial secret key generated by the KGC 'implicitly' certified the public key, the certificates are not needed [46]. Therefore, for the public key authentication process, the public key of the KGC is required.

IV. CONCLUSIONS

In this paper we investigated the position of cryptographic schemes as one of the significant security issues in mobile Ad Hoc networks.

© 2015, IJIRIS- All Rights Reserved

This investigation shows that although symmetric cryptosystems are more efficient than public key ones, a subset of advantages caused that the use of public key cryptography is more popular in resource constrained nodes of MANETs. Beside of these, security issues in mobile Ad hoc networks and different categories of public key cryptosystems and their functionality have been introduced

REFERENCES

[1] Capkun, S., Buttyan, L. and Hubaux, J.-P. (2003). Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing. 2(1), 52 – 64. ISSN 1536-1233.
[2] Douceur, J. R. (2002). The Sybil Attack. In IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems. London, UK: Springer-Verlag. ISBN 3540441794, 251–260.
[3] Yi, S. and Kravets, R. (2003). MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks. In 2nd Annual PKI Research Workshop Program. 65–79.
[4] Kim, J. and Tsudik, G. (2009). SRDP: Secure route discovery for dynamic source routing in MANETs. Ad Hoc Networks. 7(6), 1097 – 1109. ISSN 15708705.
[5] Mao, L.-Q., Ma, J.-F. and Li, X.-H. (2009). Analysis of provably secure on-demand source routing in MANET. Tongxin Xuebao/Journal on Communication. 30(1), 38 – 44. ISSN 1000436X.
[6] Xu, Y. and Xie, X. (2008). Security analysis of routing protocol for MANET based on extended Rubin logic. Sanya, China, 1326 – 1331.
[7] Yu, M., Zhou, M. and Su, W. (2009). A secure routing protocol against byzantine attacks for MANETs in adversarial environments. IEEE Transactions on Vehicular Technology. 58(1), 449 – 460. ISSN 00189545.
[8] Anjum, F. and Talpade, R. (2004). LiPaD: lightweight packet drop detection for ad hoc networks. Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. 2, 1233–1237. ISSN 1090-3038.
[9] Subhadrabandhu, D., Sarkar, S. and Anjum, F. (2004). Efficacy of misuse detection in ad hoc networks. Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on, 97–107. doi:10.1109/SAHCN.2004.1381907.
[10] Vigna, G., Gwalani, S., Srinivasan, K., Belding-Royer, E. M. and Kemmerer, R. A.(2004). An intrusion detection tool for AODV-based ad hoc wireless networks. In Proceedings - Annual Computer Security Applications Conference, ACSAC. Los Alamitos, CA 90720-1314, United States. ISSN 1063-9527, 16 – 27.
[11] Zhao S., Akshai A., Frost R., Bai X.. (2011). A survey of applications of identity-based cryptography in mobile ad-hoc networks. IEEE Commun. Surv. Tutorials Early Access.
[12] Szczechowiak P., Oliveira L., Scott M., Collier M., and Dahab R.. (2008). Nano ECC: Testing the limits of Elliptic Curve Cryptography in Sensor Networks. EWSN, ser. LNCS, vol. 4913.
[13] Perrig A., Szewczyk R., Wen V., Culler D., Tygar J. D. (2002). SPINS: Security protocols for sensor networks. In Proc. Conf. Wireless Networks, pp. 521-534.
[14] Karlof C., Sastry N., Wagner D.. (2004). Tinysec: A link layer security architecture for wireless sensor networks. In 2nd ACM Sens Sys, pp.162-175.
[15] Oliveira L.B. , Dahab R. (2006). Pairing-based cryptography for sensor networks. presented at IEEE International Symposium on Network Computing and Applications, Cambridge, MA.
[16] Gaubatz G., Kaps J.-P., Oztruk E., Sunar B. (2005). State of the art in ultra-low power public key cryptography for wireless sensor networks. In Proc. Per Sec '05, IEEE, pp. 146-150.
[17] Liu J. K., Baek J., Zhou J., Yang Y., Wong J. W. (2010). Efficient online/offline identity-based signature for WSN. In Proc. IJIS, pp. 287-296.
[18] Shamir A., (1984). Identity-Based Cryptosystems And Signature Schemes. In Advances In Cryptology—Crypto 1984, Lecture Notes In Comput.Sci. 196, Springer-Verlag, Berlin.
[19] Boneh, D., Franklin, M. (2001). Identity Based Encryption From The Weil Pairing. Advances In Cryptology—Crypto.
[20] Al-Riyami S.S., Paterson K.G. (2003). Certificateless public key cryptography. Advances in Cryptology C Asiacrypt 2003, Lecture Notes in Computer Science, pp 452-473.
[21] Eissa T., Razak S. A., Ngadi M.A. (2012). A Novel Lightweight Authentication Scheme for Mobile Ad Hoc Networks. AJSE 37. pp 2179–2192.
[22] Li L., Wang Z., Liu W. , Wang Y. (2011). A Certificate less Key Management Scheme in Moblie Ad Hoc Networks. 7th International Conf. on Wireless Communications, Networking and Mobile Computing, pp 1-4.
[23] Toh. C.K., (2002). Ad Hoc Mobile Wireless Networks Protocols and Systems. Prentice Hall,Inc.
[24] Jubin J., Tornow J.D. (1987). The DARPA Packet Radio Network Protocols", proceedings of the IEEE, vol. 75, no. 1, January 1987, pp.21-32.
[25] Fifer W. , Bruno F. (1987).The Low-Cost Packet Radio, Proceedings of the IEEE, vol. 75, no. 1, pp. 33-42.
[26] Perkins C.E. , Bhagwat P. (1994). Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers, SIGCOMM '94: Proceedings of the conference on Communications architectures, protocols and applications, ACM press, pp. 234-244.

© 2015, IJIRIS- All Rights Reserved

[27] Perkins C.E. , Royer E.M. (1999). Ad-hoc On-Demand Distance Vector Routing, WMCSA '99: Second IEEE Workshop on Mobile Computer Systems and Applications, IEEE Computer Society, pp. 90-100.
[28] Stajano F., Anderson R. (1999). The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks, In Proceedings of the 7th International Workshop on Security Protocols, LNCS 1796, Springer Verlag, pp. 172-194.
[29] Yang Y. (2014). Broadcast encryption based non-interactive key distribution in MANETs, Journal of Computer and System Sciences, Volume 80, Issue 3, pp 533-545.
[30] Guarnera, M., Villari, M., Zaia, A., Puliafito, A. ((2002). MANET: Possible applications with PDA in wireless imaging environment. In: 13th IEEE international symposium on personal, indoor and mobile radio communications, pp 2394–2398.
[31] Hoebeke J., Moerman I., Dhoedt B., Demeester P. (2004). An Overview of Mobile Ad Hoc Networks. Applications and Challenges," Journal of the Communications Network, vol. 3, pp. 60–66.
[32] Abusalah L., Khokhar A., Guizani M. (2008). A survey of secure mobile ad hoc routing protocols," IEEE Commun. Surveys & Tutorials, IEEE, vol. 10, no. 4, pp. 78–93.
[33] Hu Y., Perrig A., Johnson D. (2002). Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks. Proc. of IEEE INFORCOM.
[34] Capkun S., Buttyan L., Hubaux J., (2003). Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks.
[35] Yi S., Naldurg P., Kravets R., (2002). Security-Aware Ad-hoc Routing for Wireless Networks. Report No.UIUCDCS-R-2002-2290, UIUC.
[36] Sanzgiri K., Dahill B., Levine B., Shields C., Belding-Royer E. (2002). A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87.
[37] Hu Y., Johnson D., Perrig A. (2002). SEAD: Secure Efficient Distance Vector Routing in MobileWireless Ad-Hoc Networks. Proc. of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), pp. 3-13.
[38] Al Housani H., Baek J., Yeun CY.(2011). Survey on Certificateless public key Cryptography, Internet Technology and Secured Transactions (ICITST).
[39] Hu Y.-C., Johnson D.B., Perrig A. (2002). SEAD: Secure E±cient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks, IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp. 3-13.
[40] Hu Y.-C., Perrig A., Johnson D.B. (2002). Ariadne: a Secure On-Demand Routing Protocol for Ad Hoc Networks, MobiCom '02: Proceedings of the 8th annual international conference on Mobile computing and networking, pp. 12-23.
[41] Papadimitratos P., Haas Z. (2002). Secure Routing for Mobile Ad Hoc Networks, Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002).
[42] Adams C., Lloyd S. (2003) .Understanding Public-Key Infrastructure . Concepts,Standards, and Deployment Considerations..2nd ed,Pearson education,Boston,USA.
[43] Zhou L, Haas ZJ. (1999). Securing Ad Hoc Networks. IEEE Networks 1999; 13(6). pp 24–30.
[44] Yi S, Kravets R. (2003). MOCA: mobile certificate authority for wireless ad hoc networks. Proceedings of Second Annual PKI Research Workshop (PKI '03).
[45] Bechler M, Hof H-J, Kraft D, Pahlke F, Wolf L. (2004). A cluster-based security architecture for ad hoc networks. Proceedings of IEEE INFOCOM.
[46] Chen L., Cheng Z., Smart N.P. (2007). Identity-Based Key Agreement Protocols From Pairings .International Journal Of Information Security– Springer.

© 2015, IJIRIS- All Rights Reserved