Key Management and Distribution for Mobile Ad-Hoc Network

Jaykumar Shantilal Patel
•
Chaudhari Technical Institute, Sector-7, Gandhinagar
jay_sp_mca@yahoo.co.in

Abstract

Security has become the principal concern in mobile ad-hoc network. Secure communication depends on using cryptographic mechanisms. Cryptographic mechanism involves symmetric key and asymmetric key approaches. The symmetric key approach is more reliable except the key distribution phase. Asymmetric key approach gives robust security, but it results in high computational, high communications and high storage overhead. The propose research uses both the concepts. The symmetric key approach for reliable data exchange and asymmetric key approach for key management and distribution to achieve robust security in constraint based mobile ad-hoc network.

Keywords: Key management, Key distribution, Mobile ad-hoc network, Security.

I. Introduction

In a region where communication area and existing infrastructure is limited and inconvenience, mobile ad-hoc network is one of the solutions [1]. A mobile ad-hoc network also known as MANET is an assortment of several devices across the temporary network without any assist with the centralized administration. In such kind of network all mobile devices works as a host as well as a router. In such environment's routing protocol is required because two hosts that wish to communicate may not be capable to transmit packet directly [2]. Due to the resource constrains the nature of mobile Ad-hoc network key management is very crucial and challenging. Key management combines the security concepts like confidentiality, authentication, and key confirmation, [3]-[6] generally defines as security goals. To attain robust security, it is important to encrypt messages with strongly secure key [7]. The secure exchange of secret key is the major issue related to the symmetric cryptography implementation [8]. The asymmetric one is better than the symmetric in term of providing robust security [8]. The traditional key management schemes are insufficient for mobile Ad-hoc network. To implement ideal key management one can, have to know the basic characteristics of mobile Ad-hoc network. As well as also study the requirements of key managements.

II. Characteristics of Ad-hoc Network

Following are the core characteristics of mobile Ad-hoc network.

- ***Dynamic Topology***: Topology means physical arrangements of the node across the network. In Ad-hoc network nodes are mobile hence the topology may change frequently.

- ***Bandwidth Limitation***: Bandwidth is a transmission capacity of the network. The mobile-Ad-hoc network offer less bandwidth than traditional network. Due to this reason number of messages and packet size is limited.
- ***Energy Constrain***: All nodes across the mobile Ad-hoc networks are battery operated hence they have limited power source. Due to limited power complex algorithms may not be possible to implement in an Ad - hoc network.
- ***Physical Security***: The mobile Ad-hoc network does not have fixed infrastructure; hence nodes are being physically compromised by theft. Security is a big issue in mobile Ad-hoc network. The cryptographic key is one of the solutions of security issues. It is necessary to understand the characteristic of mobile Ad-hoc network before implementing the cryptographic key. The proposed work shows the key management in mobile Ad-hoc network.

III. Literature Review

Literature review shows that the author has studied various aspects of the key management and distribution for mobile ad-hoc networking.

The base concepts of key managements specifically covered secure communication for key materials exchange explained by Menezes et al., 1996 [9]. Based on the knowledge of neighbor discovery random key per distribution scheme for secure communication is proposed by Eschenauer and Gligor [2002] [10], the scheme is based on the exact location of the node.

Pairwise communication suggests by Pietro et al. [2003] [11]. It is based on random key assignments. The concept is later on extended to pseudo random key generation for energy efficient key management. Based on four sets of keys Zhu et al. [2003] [12] introduced a LEAP security mechanism for neighbor compromised node. Link layer key management encryption scheme TinySec proposed by Karlof et al., 2004 [13]. Hu et al., 2004 [14] presents the trusted Certificate Authority (CA) for public key cryptography. CA is responsible to revoke key as a key will compromised. Authentication is the base for secure communication [13], without robust authentication mechanism confidentiality, data integrity, and non-repudiation are hard to define. There is diversity of symmetric and asymmetric algorithms available, including DES, AES, IDEA, RSA, and EIGamal [9]. These cryptographic algorithms are the security primitives that are widely used in wired and wireless networks. They can also be used in MANETs and help to achieve the security in its unique network settings [15][16]. Asymmetric Key Cryptography is complex, slow and power hungry, and as such not at all suitable for use in ultra-low power environments [17].

The followings are the basic key management approaches used popularly in mobile Ad-hoc network. Basic Key Management, by Eschenauer and Gligor [2002] [10], Random Key Pre-distribution, by Chan et al. [2003], [18] Random Key Assignment, by Pietro et al. [2003] [11], Establishing Pairwise Keys, by Liu et al. [2003] [19], Pairwise Key Pre-distribution, by Du et al. [2003] [19] [20], Deployment Knowledge, by Du et al. [2004] [20], Group Key Management, by Eltoweissy et al. [2005], [21] Location-Based Keys, by Zhang et al. [2005] [22].

IV. Motivation

Although substantial expansions have been made towards the key management and distribution in the mobile ad-hoc network, robust security measures remain insufficient. Most of the explanation offered in literature addresses the key management and distribution in traditional network, but these may not be exactly fitted into the mobile ad-hoc network.

Thus, there is a need for a better scheme for key management and distribution in mobile ad-hoc network which can provide less computational, less communication and less storage overhead.

V. Security attacks

Compare with traditional network mobile ad-hoc network is more vulnerable to security attacks. There are two types of security attacks. One is passive and another is active [2][23][24].

- ***Passive Attack***: In passive attack intruder may not have enough knowledge to alter the captured data. The attacker only listen the communication without any kind of modification. These kinds of captures are the example of eavesdropping. These attacks break the confidentiality and are difficult to detect. Utilization of powerful encryption methods is one of the solutions of these attacks.
- ***Active Attack***: In active attack intruder may have enough knowledge to alter the captured data. The attacker listens as well as may alter the communication. These attacks break the authentication. Utilization of powerful MAC algorithms or any message digest algorithms are one of the solutions of these attacks.

VI. Key Management Requirements

Following are the base requirements for key management.

- ***Confidentiality***: Confidentiality means key information remains secrete between a source node and destination node. No one can know the key information exchange between the source and destination node. The various cryptographic algorithms are used to maintain confidentiality.
- ***Confidentiality***: Confidentiality means key information remains secrete between a source node and destination node. No one can know the key information exchange between the source and destination node. The various cryptographic algorithms are used to maintain confidentiality.
- ***Authentication***: Only the authorized nodes can gain the cryptographic key materials, no one else. The various MAC algorithms as well as message digest mechanisms are used to maintain authentication.
- ***Key-confirmation***: Key establishment protocols are responsible to ensure key confirmation. Key confirmation ensures that the key materials being exchanged are between the authorized nodes. Key confirmation uses the concepts of nonce [25].
- ***Key freshness***: It ensures new and unique independent keys are used for different sessions. The concepts of new and independent key ensure the forward and backward secrecy.
- ***Forward secrecy***: It restricts opponent from discovering subsequent keys from a compromised contiguous subset of old keys.
- ***Backward secrecy***: It restricts opponent from discovering preceding keys from a compromised contiguous subset of old keys.
- ***Key independence***: It subsumes the forward and backward secrecy. Key independence ensures that an opponent who knows a proper subset of keys cannot discover any other keys.
- ***Availability***: It ensures that whenever the network expect keying materials it is ready to use.
- ***Survivability***: Survivability is the ability of the key management to remain available even in the presence of threats and failures.
- ***Scalability***: It ensures network to allow numbers of nodes according to the requirements. The network can have the ability to add or remove nodes.
- ***Resistance***: The ability to protect against tolerates attacks.
- ***Recovery***: Ability to recover the information unavailable due to damage. The self-healing

and mutual healing mechanisms are used to implement recovery.

- ***Efficiency***: Key management schemes should be efficient in communication, computation and storage overhead

VII. Key Managements and Distribution

The basic difficulty in mobile ad-hoc network is to maintain secure communication by surroundings up secret keys between communicating nodes [1]-[6], [9]-[12]. In general this phenomenon is called key distribution [1]-[6], [9]-[12]. One of the popularly used techniques is trusted server scheme. The trusted server scheme is depends on a trusted server like karberos [Neuman and Tso, 1994] [26]. Since there is no fix trusted infrastructure in mobile ad-hoc network trusted server scheme is inappropriate [1]-[6], [9]-[13]. The second approach is based on Asymmetric and Symmetric key cryptography [27]. Asymmetric key cryptography is also known as public key cryptography. However, due to the resource constraint nature of the mobile ad-hoc deices this scheme is not much more fruitful for entire data communication [1]-[6], [9]-[16]. Asymmetric key algorithms like Diffe-Hellman [Diffie and Hellman, 1976] and RSA [Rivest et al., 1978] require high computation resources which is not feasible to transmit large amount of data in mobile ad-hoc network.

Nowadays, security is an important issue in almost every network [28]. Cryptography is a significant and dominant tool for secure communication. It transmits the cipher text across the network. The source node converts plain text into cipher text, the mechanism is known as encryption. The destination node converts received cipher text into plain text the mechanism is known as decryption. The specific key value is used for encryption and decryption. Symmetric key and Asymmetric key algorithms are used to implement the concepts of the encryption and decryption. The symmetric key algorithms use the same key for encryption and decryption. Asymmetric key algorithms use different key for encryption and decryption. So, there is no need to exchange the key value across the network. Hence it maintains the confidentiality.

The proposed scheme suggests that to use symmetric key algorithms for encryption and decryption for the data value. The problem of securely transmit key value between source and destination node will be resolved by utilizing the asymmetric key cryptography. Hence it maintains confidentiality for key exchange. Means key value is only known to intended source and destination node only.

VIII. Conclusion

After evaluating large literature, the author suggests to use Symmetric key cryptography for large amount of data. While the Asymmetric key cryptography for key exchange. This key is used for symmetric cryptography. This kind of implementation gives robust security in constraint based ad-hoc network.

References

[1] Charles E. Perkins, “Ad Hoc Networks”, Addison-Wesley, 2001.
[2] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, Wireless/Mobile Network Security, Springer, Chapter 12, 2006.
[3] M. Ilyas, “The Handbook of Ad Hoc Wireless Networks”, CRC Press, 2003.
[4] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., “Security in Mobile Ad Hoc Networks: Challenges and Solutions”, IEEE Wireless Communications, pp. 38-47, 2004.

[5] Wu, B., Wu, J., Fernandez, E., Magliveras, S., and Ilyas, M. "Secure and Efficient Key Management in Mobile Ad Hoc Networks", Proc. of 19th IEEE International Parallel & Distributed Processing Symposium, Denver, 2005.

[6] Nichols, R. and Lekkas, P, "Wireless Security-Models, Threats, and Solutions", McGraw Hill, Chapter 7, 2002.

[7] Jaykumar Shantilal Patel and Dr. Vijaykumar M. Chavda, "Robust Security Using Self-healing and Mutual-healing through Elliptic Curve in Sensor Network", International Journal of Futuristic Trends in Engineering and Technology, ISSN: 2348-4071, Volume 1, Issue 2, pp. 55-57, 2014.

[8] Jaykumar Shantilal Patel and Dr. Vijaykumar M. Chavda, "Security Vulnerability and Robust Security Requirements Using Key Management in Sensor Network", International Journal of Grid Distribution Computing, ISSN: 2005-4262, Volume 7, No. 3, pp. 23-28, 2014.

[9] Menezes, A., Oorschot, P., and Vanstone, S, "Handbook of Applied Cryptography", CRC Press, 1996.

[10] Eschenauer, L. and Gligor, V, "A key-management scheme for distributed sensor networks", In Proceedings of the 9th ACM Conference on Computer and Communication Security, Washington DC, USA, 2002.

[11] Pietro, R., Mancini, L. and Mei, A, "Random key-assignment for secure wireless sensor networks", ACM SANS, 2003.

[12] Zhu, S., Xu, S., Setia, S. and Jajodia, S, "Establishing pair-wise keys for secure communication in ad hoc networks: A probabilistic approach", In 11th IEEE International Conference on Network Protocols (ICNP'03). Atlanta, Georgia, IEEE Computer Society, 2003.

[13] Karlof, C., Shastry, N. and Wagner, D, "Tinysec: a link layer security architecture for wireless sensor networks", In Proceedings of SenSys'04, November 3-5, 2004, Baltimore, Maryland, USA, 2004.

[14] Hu, N., Smith R.R.K. and Bradford, P.G. "Security for fixed sensor networks", In Proceedings of the 42nd Annual Southeast Regional Conference, April 2-3, 2004. Huntsville, Alabama, USA, ACM Press, 2004.

[15] Nisha Sharma, Dr. Sugandha Singh, "Approaches in Key Management Schemes in Mobile Ad-Hoc Networks: A survey", IOSR Journal of Computer Engineering (IOSRJCE), Vol(18), Iss(4), pp. 10-14, Aug. 2016.

[16] J. Vijayalakshmi and Dr. K. Prabu, "Comparative Analysis of Various Routing Protocols in MANET", Proceedings of National Conf on RDEW'17, pp. 1-7, 2017.

[17] Jaykumar Shantilal Patel, "Self-Healing Sensor Network Key Distribution Scheme for Secure Communication", Research Journal of Recent Sciences, ISSN: 2277-2502, Volume 2, pp. 158-161, 2013.

[18] Chan, H., Perrig, A. and Song, D. "Random key redistribution schemes for sensor networks", In Proceedings of the IEEE Symposium on Security and Privacy, 11-14 May 2003, Oakland, California, USA, 2003.

[19] Liu, D. and Ning, P, "Establishing pairwise keys in distributed sensor networks", In Proceedings of ACM CCS '03, October 27-30, Washington DC, USA, 2003.

[20] Du, W., Deng, J., Han, Y.S. and Varshney, P. K. "A pairwise key predistribution scheme for wireless sensor networks", In Proceedings of the ACM CCS '03, October 27-30, 2003, Washington, DC, USA, 2003.

[21] Eltoweissy, M., Wadaa, A., Olariu, S. and Wilson, L. "Scalable cryptographic key management in wireless sensor networks", Journal of Ad Hoc Networks, Special issue on Data Communications and Topology Control in Ad Hoc Networks, (3) 5, September, 2005.

[22] Zhang, Y., Liu, W., Lou, W. and Fang, Y, "Securing sensor networks with location-based keys", Wireless Communications and Networking Conference (WCNC), 21-25 March 2004, Atlanata, GA, USA, 2005.

[23] Lou, W. and Fang, Y, "A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions", Ad Hoc Wireless Networks, edited by X. Chen, X. Huang and D. Du. Kluwer Academic Publishers, pp. 319-364, 2003.
[24] Murthy, C. and Manoj, B, "Ad Hoc Wireless Networks: Architectures and Protocols", Prentice Hall PTR, 2005.
[25] Jaykumar Shantilal Patel, "Strategic plan to reduce computation cost over Mobile Communication to acquire robust security", Annals of Faculty Engineering Hunedoara-International Journal of Engineering, ISSN: 1584-2665, E-ISSN: 1584-2673, Volume 18, Issue 2, pp. 53-60, May 2020.
[26] Neuman, B. C. and Tso, T, "Kerberos: an authentication service for computer networks", IEEE Communications Magazine 32(9), pp. 33-38, 1994.
[27] Jaykumar Shantilal Patel, "Security in mobile wireless network with less storage overhead", INFOCOMP Journal of Computer Science, E-ISSN: 1982-3363, Volume 19, Issue 1, pp. 26-32, June 2020.
[28] Jaykumar Shantilal Patel and Dr. Vijaykumar M. Chavda, "Sensor Network Security Issues In Each Layer", International Journal of Computer Science Engineering, ISSN: 2319-7323, Volume 2, Issue 5, pp. 258-261, September, 2013.

Received: August 27, 2020
Accepted: November 15, 2020