I J C T A, 9(28) 2016, pp. 277-282
© International Science Press

A SURVEY ON KEY MANAGEMENT IN MANET

D. Anitha* S. Aruna* Anuska Chatterjee* and Riya Khan*

Abstract: Mobile Ad Hoc Networks (MANETs) is an emerging type of wireless networking, in which mobile nodes combine on-the-spot or ad hoc basis. MANETs are self-organizing and self-healing, enabling peer-level communications between movable nodes without dependence on centralized resources or fixed communications. MANET doesn't have a central infrastructure which leads to vulnerable to attacks. Several routing protocols and trust models are used in MANET to achieve security. Various trust models are used to determine the reliability of the key management scheme to provide confidentiality, integrity, access control and availability. In this paper we present the study on various key management schemes in MANETs.

Keywords: Key management, security, mobile and ad hoc network

1. INTRODUCTION

The different components present in a network communicate with each other by means of wireless channels. With modernisation, use of wireless networks has rapidly become more popular. Wireless communication can be divided into two major types, based on network infrastructure: networks and infrastructure-less networks [1]. The most popular form of infrastructure-less network is the Mobile Ad-Hoc Networks (MANETs) which are essentially wireless networks belonging to mobile devices, which lack any well-defined infrastructure. The nodes directly communicate with each other, acting as both the host and the router. The major advantage of this form of network communication comes from its inexpensiveness, as it does not require expensive fixed infrastructures. Examples of popularly used MANETs are- Sensor networks, vehicular ad-hoc networks (VANET), among others [2]. The MANET is present on the mobile and they use wireless networks like a standard WiFi connection, cellular or satellite transmission. However, their dynamic topology makes them susceptible to various security threats. Another disadvantage of this network is that it needs to have optimised operations to provide better battery life, because these networks function on mobile battery power.

The major characteristic that makes this network so vulnerable to attacks is that a single node is responsible for the security of the entire network, especially in centralised networks. Hence, adequate security mechanisms have to be employed in MANETs, like advanced cryptographic technique. Cryptography ensures the scalability, confidentiality, integrity and availability of the network services, but gives rise to key management issues. Key management can be defined as the set of necessary techniques and procedures associated with the establishment and maintenance of keying relationship between the entities [3]. Key agreement and transport lead to key management schemes. Keying relationship is highly significant because it denotes the manner in which the nodes share information, including public and private keys.

Cryptographic techniques involve the usage of various different keys like symmetric, asymmetric/public, hybrid (symmetric + asymmetric) and group key. This paper presents the major key management schemes used in MANETs, based on the types of keys used.

* **Email:** avrlaksha@gmail.com, aruna809@gmail.com, anuskachatterjee1103@gmail.com, riyakhan.3334@gmail.com

2. SECURITY THREATS IN MANETS

The MANET is susceptible to many different forms of attack. Although, wired and other wireless networks may face the same security threats, they can be fixed easily due to the existence of a well-defined infrastructure. Attacks on MANETs can occur easily because the attacker only needs to communicate with one node, to gain access to the entire network communication system. Attacks can be categorised into- active and passive attacks. Active attacks in MANETs refer to those attacks where the misbehaving nodes have to bear some energy costs in order to perform the threat. Passive attacks are the security attacks, which arise due to the lack of cooperation with the purpose of saving energy selfishly [4]. The mobile ad hoc network is most susceptible to eavesdropping, impersonation and Denial of Service attacks. The most common form of DoS attack occurs when the attacker generates a large traffic to a specific node, consuming the device's battery and denying service to the owner. Moreover, owing to the dynamic topology of the network, nodes periodically join and leave the network, making the detection malicious nodes extremely hard. This issue is fuelled by the absence of a central control facility to monitor network traffic [5]. Hence, we have to rely on the cryptographic techniques to enhance security in MANETs, which brings us to the problems arising from key management schemes. The various key management schemes include:

3. SYMMETRIC KEY MANAGEMENT SCHEMES

In symmetric key cryptography, for both encryption of plain text and decryption of cipher text a common shared secret key is used. This shared secret key may be identical or there may be a simple transformation to go between the two keys and is shared between the sender and the receiver .every pair of communicating parties share a secret key, which means that the number of keys required is K= n*(n-1)/2 for n entities to communication.

3.1 Key Infection (INF)

R. Anderson, Chan, Haowen and Perring, Adrian [6] introduce the INF scheme where every mobile node participates equally for forming the key establishment process. INF model distributes its own symmetric key without any collaborative effort because node acts as a trust entity. It relies on real world attacker model but have weak security services. It has low operation, low storage and low encryption. This model has good resources, efficient survivability with low intermediaries and has fair scalability with the problem of late entry of mobile node. This model is simpler than other models but more vulnerable to attacks.

3.2 Distributed Key Pre-Distribution Scheme(DKPS)

DKPS is a collection of distributed cryptographic protocols that enables the node to work together as a key distributed function. Here node is not required to have a big capacity for huge key algorithm computing. It consists of three important phases, 1.Distributed key selection where every node takes a random key from the universal set by using exclusion property. For evaluating the exclusion property Cover Free Family (CFF) is used. This removes the need of Trusted Third Party(TTP) which makes MANET more dynamic.2.Secure Shared- Key Discovery(SSD) Here every node has a shared key with another node. It does not provide any security but it is easy to evaluate as eavesdropping occur here.3.Key Exclusion Property Testing (KEPT) For presenting the relationship between mobile nodes and shared keys Incidence matrix is used and for constructing this matrix binary values are used. It is used to test whether all the mobile nodes fulfil the exclusion property of CFF.DKPS needs less storage than pair-wise key agreement and is more efficient [7].

3.3 Peer Intermediateries for Key Establishments (PIKE)

This model uses trusted sensors nodes to establish the shared key and is a symmetric key agreement process using unique secret key in a set of nodes. The main idea of their approach is that it uses the concept of random key pre-distribution where each node shares a unique key with a set of nodes in 2-D , so any pair of nodes can rely on at least one intermediate node to establish the common key. [8] This scheme can be extended to 3D or other dimensions. PIKE has good security services and fair scalability.

Discussion

The PIKE model provides good security services with a good scalability but INF provides weak security for low storage cost and operations with fair scalability. DKPS model is efficient and needs less storage than the other two. There is a trade off between security and complexity so the choice of the scheme in MANET depends on the type of application. Like commercial application requires applications with less cost ,memory and power consumption and banking applications requires more security.

4. ASYMMETRIC KEY MANAGEMENT SCHEMES

Two keys are required for each node. One is the recipient’s public key, which uses transmitting node for encryption, and another is a private key, which uses the receiving node for decryption. Asymmetric key cryptography requires lesser number of keys than symmetric key cryptography. For n communicating nodes, the number of keys K=2*n, The available asymmetric key cryptography scheme are described below.

4.1 Ubiquitous and Robust Access Control(URSA)

This model uses efficient threshold cryptography algorithms to broadcast the certificate signing keys also known as tickets to all the mobile nodes. Each mobile node should have an active ticket which should be updated periodically and thus is certified and unexpired . The functionality of centralized authority is distributed among all mobile nodes existing in MANET. In order to maintain a mutual trust in network, exchanging of tickets within its neighbours takes place by a new node. In the case of single ticket granting node to avoid a single point of failure renewal of tickets are performed by the neighbour’s node.[9]

4.2 Secure Routing Protocol(SRP)

SRP is composed of three nodes and an administrative authority working as dealer for providing initial certificates. 1.Client node which are the normal user’s mobile nodes in MANET.2. Server node which is responsible for generating the partial structures and storing them in directory structure so that the mobile nodes can request for the certificates of other nodes and is a part of certificate authority. 3.Combiner Nodes lplays an important role as it combines the partial certificates from the servers into valid certificates.

4.3 Secure and Efficient Key Management (SEKM)

SEKM is a decentralized node based on a set of nodes known as server nodes which provides a detailed and safe way for interacting the coordination between secret share holders and are responsible and efficient. This model use mesh structure for server structure which consist of all servers having partial system private key to connect the server group .For providing the certificate service , the connection of the group is maintained and for share update periodic beacons are used. Maintenance cost is high[10].

4.4 Self- Organized Key Scheme (SOKS)

In this model each node is a CA as the node's public key and private key is generated by the nodes themselves. Each certificate has a validity period and should update before its expiration. It is update when the keying information is correct. For verifying the certificates a chain of public key certificates are acquired and the user verifies the first certificate then the following certificates are verified by using the public key from the previous certificates and the last certificate hols the target's public key[11].It has low scalability and resource efficiency but has high intermediates encryption operations and storage cost.

4.5 Partially Distributed Threshold CA Scheme

This scheme uses distribution of trust and threshold cryptography and is composd of n special nodes called servers. Each server has its own key pair and stores all the public keys of all nodes and of other servers in the network thus enabling them to securely communicate with each other . It is similar to SKM as it forms a partial signature using its private key but here a combiner combines all the parts of a signature and detect a compromised server. The survivability of resource efficiency is poor .

4.6 Key Distribution Technique (ID-C)

It uses threshold, ID-based cryptography i.e. a master public key is generated by the nodes in a distributed manner, during network formation. This scheme uses a master public key and a master secret key. The master public key is accessible to all the nodes in the network, while the master secret key is only available to select subset t nodes of the total n nodes in the network. The public key used for encryption is generated by the master public key and the node's ID. Similarly, the node's private key is generated by combining the node's id and the master private key. Hence, the nodes use their individual IDs as public keys and obtain the subset t shares to be combined to form private keys [12].

4.7 Identity Based Asymmetric Key Management Scheme

This key requires a trusted key generation centre, because the initiation phase involves generation of long-term public and private key pairs for the user. The generation centre randomly closes a private key for each node and its corresponding public key is released. Next, to ensure security through digital signature, each user sends his ID to the generation centre, which provides him with his unique signature. In the user verification phase, users who wish to communicate, challenge each other before generating the session keys in the key exchange phase [3].

4.7 Three Level Key Management Scheme

In order to achieve three level security this scheme combines ID-based cryptography with threshold secret sharing. Elliptic Curve Cryptography (ECC) and Bilinear Pairing Computation . It is highly secure and efficient . ECC provide small keys to mobile nodes and high security level. Key generation and Key distribution security services are done by threshold secret sharing algorithm. ECC uses 160 key and 1024 bits equivalent strength of RSA thus providing a high security level. Pairing technology provides confidentiality and authentication with less computational cost and communication overhead.[13]

Discussion

The choice of the most suitable scheme depends upon the requirements of the applications .the URSA scheme has encrypted local communication providing reliability and availability and is used for applications which requires more security like military applications. The ID-C provides scalability and good scalability, encryption , storage cost and resource efficiency against intermediate operations and thus is more used in commercial applications.

5. HYBRID KEY MANAGEMENT SCHEMES

Hybrid keys are the combination of two or more symmetric, asymmetric or symmetric and asymmetric keys. Since this scheme uses more than one key, it gives rise to more problems for MANETs. These keys are also referred to as composite keys.

5.1 Cluster based Composite Key Management

In this scheme, the network is divided into clusters and each cluster has a cluster head, which is chosen by the network administrator and is the node that can be most trusted. Public Key Generation (PKG) nodes are selected, from each cluster, which has highest trust value. The scheme uses the concept of mobile agent, hierarchical clustering and partial distributes key management. The public keys of the nodes are stored by the cluster head, which reduces the problem of PKI storage. Each node is assigned a unique ID by the CA, before it joins the network and also has a self-assigned public key. The new node which joins the network registers its information with the cluster head. The mobile agent then collects the new node information and requests certificate revocation. The public key of the cluster head is available to all the nodes in the cluster. The frequency for communication between cluster members is low and between cluster heads is high [14].

5.2 Zone Based Key Management

It uses zone routing protocol (ZRP). Each node has a defined zone. A specific predefined number is set to each mobile node, which depends on the hop distance. Each node uses symmetric key inside its zone and asymmetric key for communication across various zones. Symmetric keys are generated by Diffie-Hellman technique, whereas certificate generation takes place through threshold cryptography.

6. GROUP KEY MANAGEMENT SCHEMES

This scheme assigns a single key to a group of nodes. For a group to function on a single key, the group needs to be created and the key needs to be distributed among the group nodes [15].

6.1 Simple and Efficient Group Key Management (SEGK):

The group key is chosen by all the group members and can be changed or refreshed at regular intervals, or when the nodes in the group change. This system ensures fault tolerance by using two parallel-multicast trees called the red and blue trees. In case of the failure of one link, the other tree replaces it. Then, the intermediate keying material is distributed to the members by the group coordinator. However, this scheme assumes that all the nodes have a valid certificate from an offline configuration before entering the network.

7. CONCLUSION

MANET is one of the most significant and unique applications. Due to the absence of a well-defined infrastructure, this network lacks security and reliability of data. Thus, cryptographic techniques need to be used to secure the network, which leads to the problems of key management. Thus, key management protocols play a very important role in the study of MANETs. MANETs are highly flexible because members can join or leave the group dynamically during the whole session, providing node movement. Owing to this dynamism, the problem of key generation is further extended because this dynamic topology affects its performance. We studied in detail about the different key management schemes used in MANETs. It is found that DKPS is the most secure and efficient symmetric key management scheme, while ID based key management is the most reliable asymmetric key management scheme. Group key management scheme was discussed and is the most efficient manner of broadcasting information in a group. Hybrid key management schemes were also presented, which uses hierarchical clustering, for network extendibility and for saving network bandwidth and storage space. Following these key management schemes satisfies network security features like scalability, confidentiality, reliability, integrity and robustness of the data.

References

1. J. Wang, C. Wang and Q. Wu, Eds, "Ad Hoc Mobile Wireless Network", Beijing, National Defence Industry Press, 2004.
2. Perkins, C. (2001), "Ad Hoc Networks" Addison-Wesley.
3. A.J. Menzes, C.V.O. Paul and A.V. Scott, "Handbook of applied cryptography", CRC Press, 2010.
4. Kamanshis Biswas and Md. Liakat Ali, 'Security Threats in Mobile Ad Hoc Network' in Blekinge Tekniska Hogskola BTH.
5. Aziz B., Nourdine, E.,"A recent survey on Key Management schemes in MANET" ICTTA 2008, pp 1-6.
6. R. Anderson, Chan, Haowen and Perring, Adrian, "Key infection: Smart trust for smart dust"", !2th IEEE International Conference on Network Protocols, ICNP 2004.
7. Adlar C-F Chan, "Distributed Symmetric Key Management for Mobile Ad Hoc Networks", IEEE 2004.
8. Chan H. and Perrig A. (2005). "PIKE: Peer Intermediaries for Key Establishment in sensor Networks", in proceedings of IEEE INFOCOM.
9. L. Haiyun, K. Jiejun, P. Zerfos, L. Songwu and Z.Lixia, "URSA: Ubiquitous and Robust Access Control for mobile ad hoc networks", in IEEE Transactions on Networking, Vol. 12, No. 6, 2004.
10. Wu, B.,Wu, J.,Fernandez, E., Ilyas, M. and Magliveras, S., "Secure and efficient key management in mobile ad hoc networks", Network and Computer applications, Vol. 30, pp. 937-954, 2007.
11. S. Capkun, l. Buttyan and J.P. Hubaux, "Self-organised public key management for mobile ad hoc networks", IEEE Transaction on mobile computing, vol. 2, No. 1, 2003.
12. A. Khalili, J.Katz and W.A. Arbough, "Toward secure key distribution in secure ad-hoc networks" in Proc Applications and the Internet Workshops, 2003.
13. Wan AnXoing, Yao Huan Gong, "Secure and highly efficient three level key management scheme for MANET", WSEAS TRANSACTIONS on COMPUTERS, Vol. 10, Issue 10, 2011.
14. A.V.A Kumar and R.Pushpalakshmi, "Cluster Based Composite Key Management in Mobile Ad Hoc Networks" in International Journal for Computer Applications, Vol. 4, No. 7, 2010.
15. C.Y. Yeun, K. Han, D.L. Vo and K.J. Kim, "Secure authenticated group key management protocol in the MANET environment", Information Security Technical Report, Elsevier, Vol. 13, No. 3, pp. 158-164, August 2008.
16. ThairKhdour, Abdullah Aref, "A hybrid schema zone based key management for manets", Journal of Theorical and Applied Information technology, vol. No. ,2012.
17. Balasubramanium A., Misha S.,"Analysis of A Hybrid key management solution for ad hoc networks IEEE WCNC'05 vol 4,PP. 2082-2087,2005.
18. K. Hussain, A. H. Abdullah, S.Iqbal, K. Awan and F.Ahsan,"Efficient cluster head selection algorithm for manet", *Journal of computer science Networks and Communications*, vol. 2013, no. 7, pp. 1-7,2013.
19. R.C.W.Phan, "Fixing the integrated diffie-hellme-dsa key exchange protocol," *Communication Letters, IEEE*, vol. 9, no. 6, pp. 570-572, 2005.
20. M.Francis, M.Sangeetha and A.Sabari, "A survey of key management technique for secure and reliable data transmission in manet", *International Journal of Advanced Research in Computer Science and Software Engineering* (IJAARCSSE), vol. 3, no. 1, pp. 22-27, 2013.
21. M.Younis and S.Z. Ozer,"Wireless ad hoc networks: technologies and challenges," *Wireless Communications and Mobile Computing*, vol. 6, no. 7, pp. 889-892, 2006.
22. Bassant Selim, Chan Yeob yeun, " Key Management for the MANET:Asurvey" , International Conference on Information and Communication Technology Research,(ICTRC 2015),IEEE.
23. Renu Dalal , Yudhvir Singh and Manju Khari ," A Review on Key Management Schemes in MANET", International Journal of Distributed and Parallel Systems (IJDPS) vol.3, no.4,July 2012.