Scientific Journal Impact Factor (SJIF): 1.711
e-ISSN: 2349-9745
p-ISSN: 2393-8161
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Different Approaches for Secure and Efficient Key Management in Mobile Ad-Hoc Networks

C.Shanmuganathan[1] , Dr.P.Raviraj[2]

[1]*Assistant Professor, Department of Computer Science & Engineering, St.Peter's College of Engg. & Technology., Chennai, 600054*
[2] *Professor & Head, Department of Computer Science & Engineering, Kalaigner Karunanidhi Inst.of Tech., Coimbatore, 641402*

Abstract - A Mobile Ad-hoc Network (MANET) is a self configuring infrastructure less network of mobile devices conducted by wireless. Each device in a MANET is free to move independently in any direction and its change the link to other devices frequently. MANET includes both challenges and opportunities in achieving security goals such as confidentiality, integrity and non repudiation. Key management is a central component in MANAET security, the purpose of key management is to provide secure procedures for handling cryptography key materials. Distributed key management is proposed and deduces the condition under which the key sets distributed to the network nodes to provide MANET security. Various key management schemes are discussed for secure wireless sensor network communication. Peer Intermediaries for Key Establishment (PIKE), a class of key establishment protocols that involves using one or more sensor nodes as a trusted intermediary to facilitate key establishment. Pike protocols scale sub linearity with the number of nodes in the network and achieving higher security against node compromise than other protocols. Authenticated Routing for Ad-hoc Networks (ARAN) is proposed to detect and protect against malicious actions by third parties. ARAN has minimal Performance costs for the increased security in terms of processing and networking overhead. Self-organized Key Management is to propose cryptography procedures to make secure transactions.

Keywords - Mobile Ad-hoc Network, Key Management, Security, Key scheduling and Routing.

I. INTRODUCTION

1.1 Mobile Ad-hoc Networks (MANETs)

A mobile ad-hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore changes its links to other devices frequently. Each of the node has a wireless interface to communicate with each other. Each device must forward traffic unrelated to its own use, and therefore be a router. The major challenge in building a MANET is equipping each device to periodically maintain the information required to properly route traffic into the correct direction. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or more and different transceivers between nodes. This result causes highly dynamic, autonomous topology. A mobile ad hoc network consists of a collection of mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration.

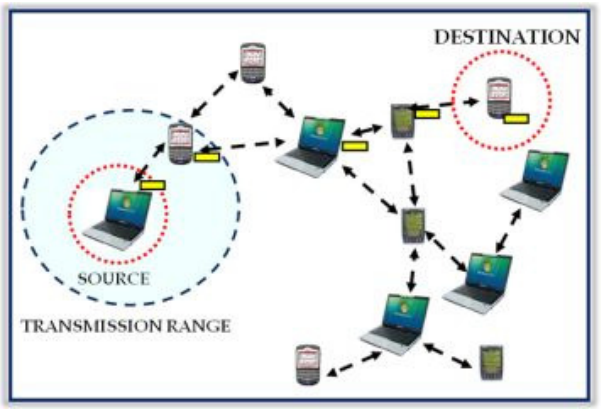

Figure 1.1 Mobile Ad-hoc Networks

1.2 Key Management

Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, storage use, exchange and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols. Key management concerns keys at the user level that is between users. This is in contrast to key scheduling; key scheduling typically refers to the internal handling of key material within the operation of a cipher. Successful key management is critical to the security of a cryptosystem. In practice it is arguably the most difficult aspect of cryptography because it involves system policy, user training, organizational and departmental interactions, and coordination between all of these elements.

1.3 Symmetric Algorithm

When using symmetric algorithms, both parties share the same key for encryption and decryption. To provide privacy, this key needs to be kept secret. Once somebody else gets to know the key, it is not safe anymore. Symmetric algorithms have the advantage of not consuming too much computing power. A few well-known examples are: DES, Triple-DES (3DES), IDEA, CAST5 and BLOWFISH

1.4 Asymmetric Algorithm

Asymmetric algorithms use pairs of keys. One is used for encryption and the other one for decryption. The decryption key is typically kept secretly, therefore called ``private key'' or ``secret key'', while the encryption key is spread to all who might want to send encrypted messages, therefore called ``public key''. Everybody having the public key is able to send encrypted messages to the owner of the secret key. The secret key can't be reconstructed from the public key. The idea of asymmetric algorithms was first published 1976 by Diffie and Hellmann. Asymmetric algorithms seem to be ideally suited for real-world use: As the secret key does not have to be shared, the risk of getting known is much smaller. Every user only needs to keep one secret key in secrecy and a collection of public keys that only need to be protected against being changed. Well-known asymmetric algorithms are RSA, DSA and ELGAMAL.

1.6 Routing in MANETs

In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path and also it forward the packets between the source and the destination. The data is forwarded between each node in ad-hoc networks. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes. Dynamic Topology: This is the major problem with ad-hoc routing since the topology is not constant. The mobile node might move or might change. In ad-hoc networks, routing tables must somehow reflect

@IJMTER-2014, All rights Reserved

these changes in topology and routing algorithms have to be adapted. Asymmetric links: Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile so the positions of nodes are constantly changed within network. Routing Overhead: In wireless ad-hoc networks, the locations of the nodes are often changed within network. So, some invalid routes are generated in the routing table which leads to unnecessary routing overhead. Interference: This is also the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

II. ASYMMETRIC KEY MANAGEMENT SCHEMES IN MANETs

2.1 Secure Routing Protocol (SRP)

In security of the entire network routing plays an important role. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. Routing security issues of MANETs, and analyze in detail one type of attack, the "black hole" problem can be easily employed against the MANETs. 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) techniques or by adjusting the configuration structure based on share redistribution techniques to handle compromised servers or system failure. Since the new shares are independent of the old ones, mobile adversaries would have to compromise a threshold number of servers in a very short amount of time, which obviously increases the difficulty of the success of adversaries. One possible solution to the black hole problem is to avoid the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. Using this method the intermediate node cannot reply, so in some sense we avoid the black hole problem and implement a secured AODV protocol. But there are two associated limitations. First, for large network the routing delay is greatly increased. Second, a malicious node will fabricate a reply message on behalf of the destination node. The source node cannot identify if the reply message is really from the destination node or fabricated by the malicious node. In this case, the method may not be adequate. We propose another solution using one more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it exists, we can trust the intermediate node and send out the data packets. If not, we just discard the reply message from the intermediate node and send out alarm message to the network and isolate the node from the network.

2.2 Routing Protocols of MANETs

Many different routing protocols have been developed for MANETs. They can be classified into two categories: Table-driven: Table driven routing protocols essentially uses proactive schemes. They attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. On demand: Source-initiated on-demand routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. Once a route is found means the process will get completed. Three main routing protocols for a MANET are destination-sequenced distance-vector routing protocol (DSDV), AODV, and Dynamic Source Routing protocol (DSR). DSDV is a table-driven routing protocol based on the classical Bellman-Ford routing mechanism.

In this routing protocol, each mobile node in the system maintains a routing table in which all the possible destinations and the number of hops to them in the network are recorded. AODV builds on the

@IJMTER-2014, All rights Reserved

DSDV algorithm described above and is an improvement since it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in DSDV. It is an on demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges.

2.3 Routing Security in MANETs

The nodes in an ad-hoc network also function as routers that discover and maintain routes to other nodes in the network. The primary goal of a MANET routing protocol is to establish a correct and efficient route between a pair of nodes so that messages may be delivered in a timely manner. If routing can be misdirected, the entire network can be paralyzed. Thus, routing security plays an important role in the security of the whole network [2].

2.4 Self-Organized Key Management

This scheme is based on the web-of-trust model that is similar to PGP. The basic idea is that each user acts as its own authority and issues public key certificates to other users. A user needs to maintain two local certificate repositories. One is non-updated certificate repository and the other one is the updated certificate repository. The reason a node maintains a non-updated certificate repository is to provide a better estimate of the certificate graph. Key authentication is performed via chains of public key certificates that are obtained from other nodes through certificate exchanging, and are stored in local repositories. The fully distributed, self-organized certificate chaining has the advantage of configuration flexibility and it does not require any bootstrapping of the system [6].

However, this certificate chaining requires a certain period to populate the certificate graph. This procedure completely depends on the individual node's behavior and mobility. One the other hand, this fully self organized scheme lacks any trusted security anchor in the trust structure that may limit its usage for applications where high security assurance is demanded. In addition, many certificates need to be generated and every node should collect and maintain an up-to-date certificate repository. The certificate graph, which is used to model this web-of-trust relationship, may not be strongly connected, especially in the mobile ad hoc scenario. In that case, nodes within one component may not be able to communicate with nodes in different components. Certificate conflicting is another potential problem in this scheme.

III. SYMMETRIC KEY MANAGEMENT SCHEMES IN MANETs

3.1 Distributed Key Pre-Distribution Scheme (DKPS)

One key idea of the DKPS is that each node individually picks a set of keys from a large publicly-known key space following some procedure so that at the end, the key patterns of all the nodes satisfy the following exclusion property with a high probability: any subset of nodes can find from their key sets at least one common key not covered by a collusion of at most a certain number of nodes outside the subset. It is aimed at the network settings where mobile nodes are not assumed to be capable of performing computationally intensive public key algorithms and the TTP is not available. The basic idea of the DKPS scheme is that each node randomly selects a set of keys in a way that satisfies the probability property of cover-free family (CFF). Any pair of nodes can invoke the secure shared key discovery procedure (SSD). The theory behind the SSD is the additive and scalar multiplicative homomorphism of the encryption algorithm as well as the property of non-trivial zero encryption [3]. To discover the common secret key, one side of the two parties can form a polynomial and send the encrypted polynomial to the other side. The coefficients of the polynomial are encrypted with the sender's secret key. The other side will send back the encrypted polynomial multiplied by a random value. Because of the homomorphism and non-trivial zero encryption properties, either side can only discover the common secret key, without disclosing the other non-common keys.

@IJMTER-2014, All rights Reserved

3.2 Peer Intermediaries for Key (PIKE)

The basic idea of PIKE is to use sensor nodes as trusted intermediaries to establish shared keys. Each node shares a unique secret key with a set of nodes. In the case of 2-Dimension, a node shares a unique secret with each of the O (n) nodes in the horizontal and vertical dimensions. It is a random key pre-distribution scheme. Therefore, any pair of nodes can have a common secret with at least one intermediate node. This key pre-distribution scheme can be extended to three or more dimensions.

IV. IMPLEMENTATION

While implementation in real world, certain changes are necessary both protocol and kernel in order to allow to operate AODV correctly. We can choose to implement AODV in Linux kernel because of inherent mobility and open loop characteristics of Linux. Protocol modifications suggest most basic changes made to AODV in route Reply and Route Table. When a node receives a route request, it replies if it either is the destination or it has a current route to the destination. In the simulation, RREPs were originally unicast from responding node to the source. As the RREP was propagated, intermediate nodes update their routing tables to include the routes to the destination. In implementation however this does not work, because if RREP is unicast from responding node to the source, the intermediate nodes use IP forwarding and do not process the packet. Additionally, a source IP address field was added to the RREP so that ultimate destination of the RREP would be retained. Similarly, AODV routing daemon communicates changes to the IP routing table through the use of net link socket. Whenever AODV has route addition, modification or deletion, it transmits a message to IP through this socket and route is updated accordingly.

Cryptographic Key generation and other techniques are established to encrypt and authenticate the messages that are transferred through various wireless networks. The security of this network completely depends on the mode of key utilized to a particular network. Using a single shared key for the entire network that runs more number of applications is not secure. Therefore, pair-wise key generation using some of the well-known cryptographic techniques can be used to authenticate the network from unauthorized user [7]. The utilization of the traditional pair-wise key such as public key is not suitable for sensor nodes due to resource constraints. In such a case, the main challenge is to find an efficient way of distributing keys and keying materials to sensor nodes prior to deployment. A different pair-wise key distribution schemes have been developed for peer-to-peer wireless sensor networks and hierarchical wireless sensor networks. The problem of how resources can effectively be used to distribute session keys is referred to as the group key distribution problem. The group key distribution problem has been studied extensively in the larger context of key management for secure group communications, mainly on balancing the storage complexity and the communication complexity [4].

PIKE is dependent on having a globally addressable communication infrastructure in place prior to the establishment of security. Geographic distance can be computed easily as an estimate of the routing cost to any potential intermediary, and the locations of arbitrary nodes can be discovered efficiently via a geographic hash table (GHT). In general, however, any globally addressable communications infrastructure could be used in place of geographic routing. Because we assume that sensor nodes are immobile, GHT is slightly modified to provide a more efficient structure for the dissemination of location information [5]. The hierarchical structure of GHT is removed in favor of a uniform dissemination network since the data in this case has only one source and is unchanging; hence there are no data consistency issues.

@IJMTER-2014, All rights Reserved

V. CONCLUSION

In this paper, ARAN provides a solution for secure routing in the managed-open environment. ARAN provides authentication and non-repudiation services using pre-determined cryptographic certificates that guarantees end-to-end authentication. Attack detection and defense mechanism is proposed by using both the route redundancy in ad hoc networks and the message redundancy in topology discovery of the routing protocols. MANET's security is the challenging issue in providing authentication. Single shared key for many applications may raise problems in ensuring authentication. The approach of employing distributed key scheme for MANET ensures the network security. This paper discusses on different cryptographic key generation techniques that are proposed in literature. Some of the techniques described are Symmetric Key Cryptography, Digital Certificates, and Threshold Cryptography. PIKE enjoys a uniform communication pattern for key establishment, which is hard to disturb for an attacker. The distributed nature of PIKE also does not provide a single point of failure to attack, providing resilience against targeted attacks. In contrast to the currently popular random-key pre distribution mechanisms, PIKE have the advantage that key establishment is not probabilistic, so any two nodes are guaranteed to be able to establish a key.

REFERENCES

[1] Y. Zhang, J. Zheng," A Survey of Key Management in Mobile Ad Hoc Networks", Handbook of Research on Wireless Security, pp. 1-23, 2006.

[2] Kimaya Sanzgiri, Bridget Dahill," A Secure Routing Protocol for Ad Hoc Networks", University of California, pp.1-10, 2002.

[3] J. Wu and R. Wei," Comments on "Distributed Symmetric Key Management for Mobile Ad hoc Networks", from INFOCOM 2004.

[4] N. Vimala, R.Balasubramaniam," Distributed Key Management Scheme for Mobile Ad-Hoc Network-A Survey", Global Journal of Computer Science and Technology, Vol. 10, Issue 2, pp.7-11, April 2010.

[5] Haowen Chan, Adrian Perrig, "PIKE: Peer Intermediaries for Key Establishment in Sensor Networks", 2004.

[6] K.Nikhila Reddy, N.Naresh Reddy, Dr.P.Raja Prakash Rao ," Self-Organized Trust-Based Public-Key Security Management for Mobile Ad Hoc Networks", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 5, September- October 2012.

[7] W. Du, J. Deng, Y. S. Han, and P. K. Varshney,"pairwise key predistribution scheme for wireless sensor networks", in Proc. 10th ACM Conference on Computer and Communications Security, Oct. 2003, pp. 42-51.

@IJMTER-2014, All rights Reserved