Cipher Suites - The Cryptographic Computations in Routing of Mobile Ad hoc Networks (MANET)

J Rajeshwar[1], **G Narsimha**[2]

[1]Research Scholar, Department of Computer Science and Engineering, JNTUHCE, JNTUH,
Kukatpally, Hyderabad A.P, India
prof.rajeshwar@gmail.com

[2]Assistant Professor in CSE, JNTUH College of Engineering, JNTUH,
Kukatpally,,Hyderabad, A.P, India
narsimha06@gmail.com

Abstract: ***A mobile ad hoc network (MANET) is an infrastructure less and autonomous network where a set of nodes are connected by wireless links where each node works as both a router and an end system. Due to vulnerable features of MANET it is prone to several attacks from insider as well as outsider, so security is a major requirement for this it is using several cipher suites in order to have a strong security features. In my research cryptographic computations are playing vital role for that reason in this paper we want to discuss the various available cipher suites and the various cryptographic functions. And mainly discuss the various secure routing protocols that how they are using cipher suites. Routing is one of the basic networking functions in mobile ad hoc networks for that reason especially we are concentrating on routing security of a MANET and role of cipher suites in providing security to the routing of a MANET***.

Keywords: MANET, Cipher Suite, Cryptographic Computations, Hash functions.

1. Introduction

1.1 MANET and its Routing

Ad hoc networks change the current scenario of communication. The concept of ad hoc network allows the wireless devices to communicate without any central server or access point. Ad hoc network are very much flexible and adaptable to the needs and requirement of the data traffic travel throughout the network. The network infrastructure is not fixed in such kind of networks, as the nodes involve in these networks are movable and also the participation of the nodes is ad hoc. In ad hoc networks each node can move into the network and leave it at any point of time. Mobile nodes that are within each other's range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers [1]. Each node guides the routing messages according to the routing protocol designed for such kind of networks.

Ad hoc networks rely on multi-hop wireless communications where nodes have essentially two roles: (i) acting as end-systems and (ii) performing routing functions. A routing protocol is used to determine the appropriate paths on which data should be transmitted in a network.

Routing protocols for wireless systems can be classified into topology-based protocols and position-based ones:

• **Topology-based protocols** rely on traditional routing concepts, such as maintaining routing tables or distributing link-state information

• **Position-based protocols** use information about the physical locations of the nodes to route data packets to their destinations.

Topology-based protocols can be further divided into proactive protocols and reactive ones

• **Proactive routing protocols** try to maintain consistent routing information within the system at any time.
• **In reactive routing protocols**, a route is established between a source and a destination only when it is needed. For this reason, reactive protocols are also called on-demand protocols.

This paper is organized in the following way chapter 1 describes about the introduction of MANET and it routing, chapter 2 tells about cipher suite and cryptography, chapter 3 describes the various secure routing algorithms which are using the cipher suite and the chapter 4 describes the hash functions and chapter 5 with conclusion.

2. Related Work

2.1 Vulnerabilities of MANET and Cipher Suite

Due to openness and dynamic topology of MANET it is more prone to attacks from different ends, in this insecure environment routing becomes challenging task, for this reason many routing protocols adapted cipher suites to have a security.

Many basic routing protocols like AODV have been given security to the routing by adding cipher suites feature.

Cipher suite is nothing but a collection of cryptographic algorithms which are used to provide security feature like confidentiality, authentication, access control, non repudiation, integrity and availability.

Cryptography is the process of encryption and decryption used to provide security services. During transmission of a information it is converted in to unreadable form called cipher text and this process of converting plain text into cipher text is called encryption and the reverse process of encryption is called decryption.

There are two types of cryptographic algorithms one is symmetric (private key) algorithm and other is asymmetric (public key) algorithm. These algorithms play a vital role in providing security not only to the data but also for routing protocols.

Symmetric cryptographic algorithms fall into two categories block ciphers and stream ciphers. The block ciphers are DSE,AES, Blowfish, Triple DES, Serpent , Twofish, Camellia, CAST-128, IDEA, RC2, RC5, SEED, Skipjack, TEA, XTEA and the stream ciphers are RC4, A5/1,A5/2, FISH ,ISAAC, MUGI, Panama, Phelix, Pike, Py QUAD, Scream, SEAL, SNOW, SOBER, SOBER-128, VEST, WAKE

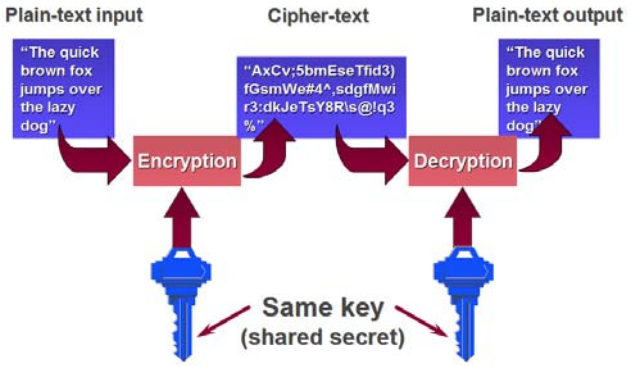
Plain-text input
Cipher-text
Plain-text output
"The quick brown fox jumps over the lazy dog"
"AxCv;5bmEseTfid3)fGsmWe#4^,sdgfMwir3:dkJeTsY8R\s@!q3%"
"The quick brown fox jumps over the lazy dog"
Encryption
Decryption
Same key
(shared secret)

Figure 1: Symmetric cryptography

The most popular asymmetric cryptographic algorithms RSA, Diffie Hellman key exchange algorithm, DSS, ElGamal and Rabin cryptosystem

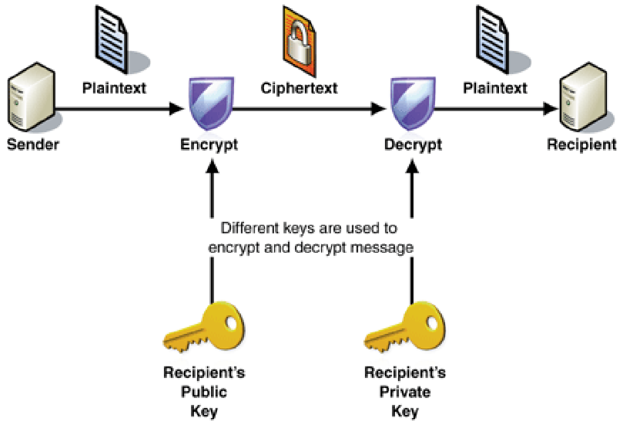

Figure 2: Asymmetric cryptography

A variant of these algorithms are MAC algorithms which also play an important role in the security of a routing protocol. The most variant of the MAC algorithms is one way hash algorithms like SHA-1, MD-5, HMAC and Whirlpool are now a day's mostly used in the cipher suites.

Digital certificates like Kerberos and X.509 are important part of security system build using the above mentioned symmetric and asymmetric algorithms.

3. Secure Routing Algorithms

3.1 Secure routing and the usage of cipher suites.

We are having many secure routing algorithms to protect MANET and its routing. The most popular routing algorithm identified by IETF for MANET is AODV, it is modified by many researchers to add security capabilities. In trusted environment AODV performs well but in the malicious, selfish and compromised environment it is prone to many attacks for that reason it added with security capabilities using variant cipher suites. The algorithms which used cipher suite are Secure AODV (S-AODV) [2], Secure Routing with AODV (SRAODV), Adaptive Secure AODV (A-SAODV) [3], Authenticated Routing for Ad hoc Networks (ARAN) [4], AODV Security Extension (AODV-SEC) [5] and so on.

3.2 SAODV

It uses digital scheme for authentication in which it is using HMAC algorithm and one way hash chain. It uses public key cryptography for key exchange.

3.3 ARAN

It is using the public key cryptography for security services. It is using public and private secret key pair for each node.

3.4 Ariadne [6]

It uses secret MAC keys between sender and receiver, for authentication it uses MAC algorithm. It uses TELSA (Time Efficient Stream-Loss Tolerant Authentication) keys for authentication of messages; hash chains are used to generate these keys.

3.5 A-SAODV

It uses multithreaded application in which a dedicated thread is used for cryptographic operations to provide security services.

3.6 SEAD (Secure Efficient Ad hoc Distance Vector Routing Protocol) [7]

It is using one way hash function for authenticity of data packets and the hash chain value for routing update.

3.7 SRP (Secure Routing Protocol) [8]

It is using the security association (SA) between the source node and the destination node. It uses the shared secret key and MAC for authentication.

4. Hash Functions

4.1 Hash functions and MAC

Hash functions are playing vital role in secure routing algorithms to provide security services like message authentication and integrity.

A Hash function is a function **H: {0, 1}* →{0, 1} ^{n}** that maps arbitrary long messages into a fixed length output.

x → (input) message.
y = H(x) (hash value, message digest, fingerprint).

The hash value of a message can serve as a compact representative image of the message (similar to fingerprints). Examples: MD5, SHA-1, SHA-256

Message Authentication Code (MAC) is another variant of hash function which is also used to provide message authentication as well as integrity.

A MAC function is a function **MAC: {0, 1}* x {0, 1}^{k} → {0, 1}^{n}** that maps an arbitrary long message and a key into a fixed length output, it can be viewed as a hash function with an additional input (the key), the sender computes the MAC value M = MAC(m, K), where m is the message, and K is the MAC key the sender attaches M to m, and sends them to the receiver the receiver receives (m', M'), the receiver computes M" = MAC (m', K) and compares it to M', if they are the same, then the message is accepted, otherwise rejected after successful verification of the MAC value, the receiver is assured that the message has been generated by the sender and it has not been altered. Examples: HMAC, CBC-MAC schemes

5. Conclusion

In this research paper we have introduced the MANET, its vulnerabilities and also the types of routing, we have briefly explained the concept of cipher suite i.e. cryptography and the types of cryptography with its importance in securing the MANET, especially routing. Finally we have the secure routing algorithms which are using the cryptography in order to provide security services to the MANET routing. We have to further explore deep into the various approaches of cryptography in order to have a robust security services

References

[1] L. Zhou and Z.J. Haas, "Securing ad hoc networks", IEEE Network Journal, November-December 1999, 13(6), pp. 24-30.

[2] Manel Guerrero Zapata:"Secure Ad hoc On-Demand Distance Vector (SAODV) Routing" INTERNET-DRAFT draft- guerrero-manetsaodv-06.txt. september 2006.

[3] Davide Cerri and Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", 0163-6804/08 © 2008 IEEE, IEEE Communications Magazine, February 2008

[4] Abdalla Mahmoud Ahmed Sameh Sherif El-Kassas, " Reputed Authenticated Routing forAd Hoc Networks Protocol (Reputed-ARAN)" 0-7803-9466-6/05/$20.00 ©2005 IEEE

[5] Stephan Eichler and Christian Roman, "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC",1-4244-0507-6/06/$20.00©2006 IEEE

[6] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks." In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (ACM Mobicom), Atlanta, Georgia, September 23 - 28, 2002

[7] Yih-Chun Hu ,David B. Johnson , Adrian Perrig "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks",1570-8705/$ 2003 Published by Elsevier B.V. doi:10.1016/S1570-8705(03)00019-2

[8] Yih-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing" ,May-June 2004@IEEE