International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review on Security Issues and Encryption Algorithms in Mobile Ad-hoc Network

Deepti Ranaut[1], Madal Lal[2]

[1, 2] Department of Computer Engineering, Punjabi University Patiala, India

Abstract: ***Now-a-days in wireless devices, Mobile Ad-hoc Network become an important part for communication for mobile devices. Mobile Ad-hoc Networks (MANETs) allow wireless nodes to form a network without requiring a fixed infrastructure. Due to the absence of the central infrastructure, we face many challenges or problems during sending data from one mobile node to another mobile node. In this paper, we discuss about features of MANET, their advantages and disadvantages and security issues and their solutions in the mobile ad-hoc network. Cryptography is the way of hiding information during transmission over a channel. There are lots of cryptographic algorithms available to protect our data from intruders.RSA also one of the effective public key cryptographic algorithm which needs time and memory.***

Keywords: Mobile Ad-hoc Network (MANET), Attacks, Cryptography, AES, DES, RSA, MD5, DSA

1. Introduction

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes without having a pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. Nodes participating in the network do not rely on a fixed infrastructure, but use each other to communicate outside their own transmission range. The nodes may join and leave the network at arbitrary points in time. Due to the mobile nodes, results changes in the network topology. Such network finds application in personal area networking, meeting rooms and conferences, emergency operation, disaster relief and military operation. In MANET, each node acts both as a router and as a host & even the topology of network may also change rapidly.

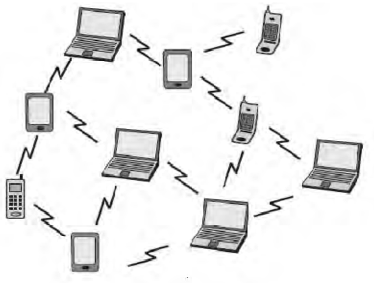

Figure 1: Structure of MANET

Characteristic of MANET:

- Nodes act as host or router.
- MANET is capable of multihop routing.
- Nodes can join or leave the network any time, it make network topology dynamic in nature.
- In MANET mobile nodes are characterized with less money, power and light weight feature.
- Wireless links are particularly more vulnerable to eavesdropping, spoofing and denial of service (DOS) attacks.
- It has high density mobility for number of users.
- It has robust and low cost network.
- Wireless connectivity among nodes are bandwidth constrained.

Challenges in MANET:

- It has limited wireless transmission range.
- Wireless links are times varying in nature.
- It has Packet losses due to error and node mobility in transmission.
- Mobility induced route changes in routing problem.
- It has security problem during transmission of data.
- It has frequent network partitions.
- It has Battery constraint energy efficiency problem.

2. Security Criteria in MANET

In this section, we have discussed different security criteria with reference to mobile ad-hoc networks.

- **Availability**
  It refers to the property of the network to continue provide services regardless of the state of the network. A denial of service attacks is based to attack this property [9].
- **Integrity**
  Integrity guarantees that no modification, addition, deletion is done in the message, the altering of message can be done malicious or accidental [9]. It assures that the data received are exactly same as sent by an authorized entity.
- Confidentiality
  It allowed that the message cannot be even viewed in its original form by any unauthorized person. The transmitted message must make sense to only the intended receiver.
- **Authenticity**
  With the help of this property, the sender and receiver prove their identities. This property ensures that the parties are genuine not impersonators or intruders.
- **Non repudiation**
  With the help of this property the sender and receiver cannot be able to deny about sending and receiving the message [10].

- **Authorization**
  This property assigns different access rights to the different types of the users. For example, a network management can be performed by network administrator only.

3. Attacks on Layers

Layers	*Attacks*
Application	Malicious Code ,Repudiation
Transport	Flooding
Network	Black Hole, Grey Hole, Worm Hole
Data Link	Internal, External
Physical	Eavesdropping, Traffic Jamming
All	DOS

3.1 Attacks in MANETs

There are two types of attacks in the MANET. First is the internal attack and second is the external attack. An external attacks causes congestion, sends false routing information or causes unavailability of services. In an internal attack, the malicious node from the network gains unauthorized access and impersonates as a genuine node .It can analyze traffic between other nodes and may participate in other network activities [9], [10].

Denial of Service attack: This attack prevents the normal use or management of communications facilities. This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available to the actual recipients. The attacker generally uses the radio signal jamming and the battery exhaustion method [7].

Impersonation: Impersonation attack is a severe threat to the security of mobile ad hoc network. If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information of the users.

Eavesdropping: Eavesdropping [10] is another kind of attack that usually happens in the mobile ad-hoc networks. This is the passive attack. The node simply observes the confidential or personal information. This information can be later used or misuse by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized or attacker access.

Routing Attacks*:* Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad-hoc networks, attacks against routing are generally classified into the two categories: attacks on routing protocols and attacks on packet forwarding/delivery [4]. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on the packets forwarding try to disturb the packet delivery along a predefined path.

4. Security Solutions in MANET

In this section we discuss security solutions to deal with the attacks describes in the previous sections. There are two general solutions to avoiding such attacks, using IDSs and cryptography.

In the first solution all nodes or some of them are equipped with intrusion detection system (IDS) in order to detect the intrusions and then isolate the adversary nodes from the network. One of the disadvantages of IDSs is that the detection of the intrusions is not a deterministic task, so there exists a large number of false positives and false negatives in the detections. Also according to the wireless nature of MANETs, using such a mechanism cannot prevent eavesdropping, therefore cannot achieve confidentiality. Hence, using IDSs is not a complete solution for securing MANETs [1].

The second solution for providing security within MANETs suggests encrypting the message before sending it i.e. Cryptography [1] .Cryptography enables the user to transmit confidential information across any insecure network so that it cannot be used by an intruder. Cryptography is the process that involves encryption and decryption of text using various mechanisms or algorithms. There are two general categories of cryptographic algorithms. The first one is named Symmetric Key Cryptography which defines a shared key between each pair of nodes. If all shared keys are the same, the method will be called Shared Key Cryptography. Examples include DES and AES. But symmetric-key cryptography has some limitations. One major limitation is the key distribution problem. In this method, compromising each node results in destroying security in the whole network. The second cryptographic algorithm is called Asymmetric Cryptography. In this kind of cryptography each node has two keys, public key and private key. The public key of each node is public for any node and the private key is known only by the owner of the key. Here, if a node wants to send a message to another one, it should encrypt the message by the destination node’s public key. The encrypted message will not be decrypted other than with the private key that is known just by the destination node. In different networks that use asymmetric cryptography, there exists a third party or a group of distributed third parties that produces an infrastructure. As discussed before, MANETs do not have any infrastructure or server, so there is no third party. Using asymmetric cryptography in MANETs without third party or any other infrastructure, leads to store the public keys of all nodes in every one.

4.1 Encryption Algorithms

DES (Data Encryption Standard): The Data Encryption Standard is the one of the first commercially developed ciphers. DES is the result of efforts done by IBM (International Business Machines) corporation, NBS (National Bureau of Standards) and NSA (National Security Agency). DES is the block cipher that encrypts 64-bit data blocks and encryption of the data is performed using a 56-bit secret key [4]. DES consists of sixteen rounds and two permutation layers. DES uses a shared key both to encrypt and decrypt the message. The decryption process is the reverse of encryption process. DES possesses strong Avalanche effect and is flexible as it works in CBC, ECB, CFB and OFB modes. DES easily falls prey to Brute Force attack and relatively slow in software [3].

AES (ADVANCED ENCRYPTION STANDARD): AES [6] can process the 128 bit data blocks and uses key lengths of 128, 192, or 256 bits. For the key length of 128,192 and 256 bits, AES may be known to as AES-128, AES-192 and AES-256 respectively. Unlike DES, AES is not a fiestel structure. Number of rounds in AES depends on key length i.e. for a key length of 128, number of rounds is 10 and similarly for 192 and 256 bit keys, it is 12 and 14 respectively. AES provides security against all known attacks, simple in the design and good speed of computation.

The problems of key distribution are solved by public key cryptography. Some examples of the public-key cryptosystems are: RSA, Diffie-Hellman and DSA.

RSA (Rivest, Shamir and Adleman): A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. It is widely used in electronic commerce protocols, and is believed that its security depends on the difficulty of decomposition of large numbers. RSA [2] is secure because it is able to resist concerted attack. RSA [5] was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key encryption.

Diffie-Hellman: Whitfield Diffie and Martin Hellman discovered Diffie-Hellman (DH) algorithm in 1976 was the first public key algorithm ever invented. Diffie–Hellman [3] establishes a shared secret key that can be used for secret communications by exchanging data over a public network. Diffie–Hellman algorithm does not need any known key before communication begins and Discrete Logarithm Problem makes it extremely difficult to crack. Diffie–Hellman algorithm easily falls pray to man-in-the-middle attack [3].

DSA (Data Signature Algorithm): Data Signature Algorithm as an approved signature scheme was invented by David Kravitz. Digital Signature Standard (DSS) used DSA proposed by National Institute of Standards and Technology (NIST) in 1991. Security of DSA [6] is based on the difficulty to solve discrete logarithms. DSA has been accepted widely. DSA is more efficient and faster than RSA [8].

Hashing Algorithm: The MD5 message-digest algorithm is the widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. An MD5 hash is typically expressed the hexadecimal number, 32 digits long. MD5 processes a variable-length message into the fixed-length output of 128 bits. The input message is divided into the chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512 [11].

5. Conclusion

This paper presents the detailed study of the popular Encryption Algorithms such as DES, AES, RSA, Diffie-Hellman, DSA and hashing algorithms. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide more security to the network and data, different encryption methods are used. In this paper, a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which is suitable for different applications and has its own advantages and disadvantages. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. Our future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to secure the data during transmission from intruders and other attacks in mobile ad-hoc network.

References

[1] Mohammed Gharib, Ehsan Emamjomeh-Zadeh, Ashkan Norouzi-Fard and Ali Movaghar, “A Novel Probabilistic Key Management Algorithm for Large-scale MANETs”, IEEE,27th International Conference on Advanced Information Networking and Applications Workshops,2013

[2] Athulya M S,Sheeba V S, "Security in Mobile Ad-Hoc Networks",IEEE-20180,ICCCNT'12,26th -28th July 2012

[3] Veerpal Kaur,Aman Singh, "Review of Various Algorithms Used in Hybrid Cryptography", International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013

[4] Ajay Kushwaha,Hariram Sharma, "Enhancing Selective Encryption Algorithm for Secured MANET", IEEE, Fourth International Conference on Computational Intelligence, Modelling and Simulation,2012

[5] Khushdeep Kaur, Er. Seema, “Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices”, International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September- October 2012

[6] Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, “DSAB – A Hybrid Approach for Providing Security in MANET”, INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, Vol.1, No.3

[7] Jayashree.A.Patil,Nandini Sidnal, "Survey - Secure Routing Protocols of MANET", International Journal of Applied Information Systems (IJAIS),Volume 5– No.4, March 2013

[8] Amol Bhosle, Yogadhar Pandey, "Review of authentication and digital signature methods in Mobile ad hoc network", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),Volume 2, Issue 3, March 2013

[9] Rashid Sheikhl, Mahakal Singh Chandee, Durgesh Kumar Mishra, "Security Issues in MANET:A Review",IEEE,2010

[10] Wenjia Li,Anupam Joshi, "Security Issues in Mobile Adhoc Networks:A Survey"

[11] Edna Elizabeth N., Subasree S., S. Radha,"Enhanced Security Key Management Scheme for MANETS", WSEAS TRANSACTIONS on COMMUNICATIONS,Volume 13, 2014