A REVIEW ON DATA SECURITY USING PGP & DES

Vikas Gupta[1], Harprabhdeep Singh[2]
[1, 2]Adesh Institute of Engineering & Technology
Faridkot

Abstract: Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks, because of features like open medium, changing topologies, lack of central monitoring and management of cooperative algorithms and no clear defense mechanism. Hence the proposed review has been attempted to study the vulnerability of MANETs against security attacks and find the appropriate techniques.
Keywords: PGP, DES, Data Security, MANET

I. INTRODUCTION

In recent years, much interest has been involved in the design of Mobile Ad-hoc Network (MANET) technologies. Mobile ad-hoc networks are characterized by their self-configuration, open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These characteristics make them vulnerable to security attacks. Existing security solutions for wired or wireless networks with infrastructure cannot be directly applied to MANETs. Designing security solutions for MANET is the nontrivial challenges. The goal of security solutions is to provide security services, such as authentication, confidentiality, integrity, and availability to mobile users. In order to achieve this goal, we must develop some key management systems adapted to the characteristics of MANET.

A. MANET

An ad-hoc network is a collection of wireless mobile hosts forming an impermanent network without the assistance of any stand-alone infrastructure or centralized administration. As shown in Fig 1, Mobile Ad-hoc networks are self-configuring and self-organizing multi-hop wireless networks. Each node in mobile ad hoc networks is set up with a wireless transmitter and receiver, which permits it to communicate with other nodes in its communication range only. Nodes communicating usually share the similar physical media; they transmit and get signals at the same frequency band, and follow the same hopping sequence or spreading code. If the destination node is not inside the transmission range of the source node, the source node takes help of the intermediate nodes in order to communicate with the destination node by relaying the messages hop by hop.

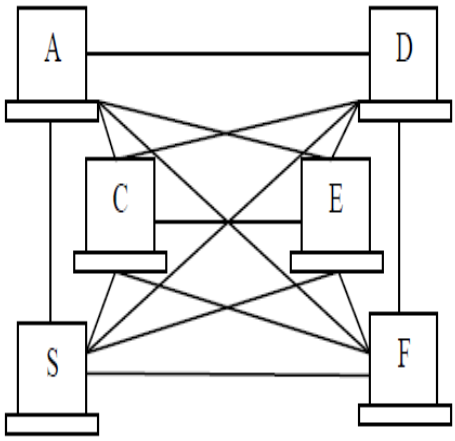

Fig 1 Mobile Ad hoc Network (MANET)

Fig1 illustrates the Mobile ad-hoc network. In order for a node to transmit a message to a node that is out of its radio range, the cooperation of other nodes in the network is required; this is called as multi-hop communication. Therefore, each node at the same time must act both as a host and as a router as well. Mobile Ad-Hoc network is an autonomous system, where nodes/stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. Mobile Ad-Hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes the mobile Ad-Hoc networks unpredictable from the point of view of scalability and topology.

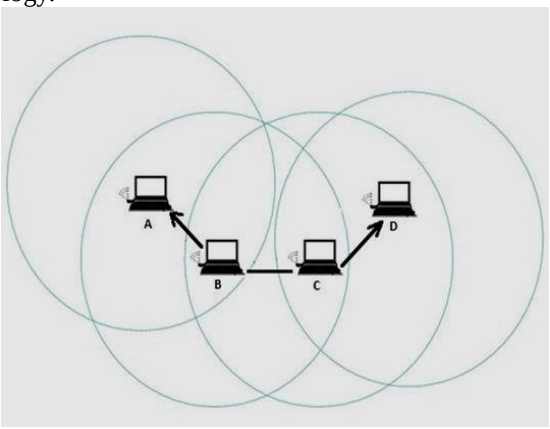

Fig 2 Mobile Ad hoc Network

B. Security of DES

This secret key encryption algorithm uses a key that is 56 bits, or seven characters long. At the time it was believed that trying out all 72,057,594,037,927,936 possible keys (a seven with 16 zeros) would be impossible because computers could not possibly ever become fast enough. In 1998 the Electronic Frontier Foundation (EFF) built a special-purpose machine that could decrypt a message by trying out all possible keys in less than three days. The machine cost less than $250,000 and searched over 88 billion keys per second

C. PGP Algorithm

PGP (Pretty Good Privacy) is a security algorithm in wireless sensor network. It is used to provide security in database. It is most widely used standard in the world for securing electronic mails. It provides confidentiality, integrity and authentication to its users. These security services are provided at a cost of various cryptographic algorithms. Given a data, choosing particular algorithms for its security, according to the user requirements, is a non-trivial task. PGP is an example of lightweight encryption algorithm. Lightweight encryption algorithms are employed in hand held devices, low power operating systems and low power wireless sensor networks because they take less time for encrypting video data. Encryption is a process of converting plaintext that is understood by human to cipher text that is understood by machine. When using PGP algorithm the key pair is generated. One key of the pair is the Private Key which should always be kept safe and never given to anyone. The other key is the public key which should be given to as many people as possible. PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and, finally, public-key cryptography, each step uses one of several supported algorithms. Each public key is bound to a user name and/or an e-mail address. PGP is a powerful application providing security for files and for e-mail. In addition to PGP, there is also GNU Privacy Guard, also Known as GPG (or gnupg). PGP is a powerful application providing security for files and for e-mail. At the heart of PGP is something called a "PGP key?" A PGP key is really a key pair, which consists of a private key and a public key. The term "PGP key" almost always refers to the public key part of a key pair. A PGP key is either an "RSA key" or a "DSA key." These terms refer to cryptographic algorithms. Each algorithm offers excellent security. Until the year 2000, DSA was much more popular than RSA because the RSA algorithm was encumbered by a patent. That patent expired September 17, 2000. Since then, RSA has become much more popular than DSA. A key length of at least 1024 bits should be specified for either RSA or DSA. As of 2005, 512 bit RSA keys are considered insecure; 768 bit keys are considered secure, but security experts recommend that new keys should be at least 1024 bits long. (The longer the key, the harder it is for a stranger to "crack" the key, or discover the private part of the key pair. Once someone has the private key, that person can impersonate you without anyone's knowledge.) A public key is basically a big number. For example, a 1024-bit public key is a 308 digit number. (i.e. 1 followed by 307 zeros:

People don't remember numbers that big, but computers can handle them quite nicely. People do remember names and e-mail addresses as identities. So, a UID (user identity) defines to whom this public key belongs. In general, in cryptography, the term "signature" refers to something being used as private key. As in the pen and paper of the physical world, a document is signed by feeding that document along with the private key to the "signing algorithm" (either RSA or DSA). Someone who wants to check the signature on a document feeds the document, signatures, and related public key to the signing algorithm. The signing algorithms will then either say that "the signature is verified" or "the signature could not be verified." If the signature could not be verified, there are two possible reasons. Either someone altered the document after it was signed, or someone tried to "forge" the signature without the private key. This is why it is essential to keep private key private. Anyone who has access to the private key can generate signatures. For Example**:** Suppose Alice creates a user identity that says "I'm Alice, and my e-mail address is alice@alice.com." Now, Bob knows Alice, so Bob is willing to vouch for Alice's identity. Bob gets Alice's public key from her. Bob then creates a certificate that says "I, Bob, state that this identity for Alice is correct and that this public key belongs to Alice." Bob signs this certificate with his private key. Bob then adds this signed certificate to Alice's public key and sends the revised key back to Alice. Now, when Alice gives out her PGP public key to Carol, Carol can check Bob's signature on the certificate. If the signature verifies correctly, then Carol knows that Bob has vouched for Alice's identity. The simplest PGP key contains the following items:

- The public key itself
- The user identity (UID)
- A certificate corresponding to the UID.

A key contains the public key itself and a user identity. But why is there a certificate following the UID, and who creates the certificate? Suppose there were no certificate. Then, suppose Alice creates a new PGP key. This key contains the public key portion of the RSA or DSA key pair and the UID that says "This key belongs to Alice (alice@alice.com)." Let's suppose Mallory is a malicious prankster who wants to deface Alice's key. What prevents Mallory from replacing the UID with one that says "This key belongs to Mallory (mallory@mallory.com)"? That's the purpose of the certificate. Alice creates a certificate that says "I'm Alice, and I'm asserting this key belongs to Alice (alice@alice.com)." Alice signs the certificate with the private key. Then, anyone who uses this PGP key can check Alice's signature with the public key to verify the UID hasn't been tampered with. Because Mallory does not have access to the private key, his attempt to deface Alice's PGP key will fail. When a new PGP key is generated, PGP asks for a name and an e-mail address to be included in the key. PGP uses this data to create the UID for the new key. PGP also creates the certificate for the UID automatically.

II. LITERATURE REVIEW

Haas (2003) in the paper "Secure Data Transmission in Mobile Ad Hoc Networks" presented an approach on Secure Message Transmission in Mobile Ad hoc Network. The security of data transmission is achieved without restrictive assumptions on the network nodes' trust and network membership, without the use of intrusion detection schemes, and at the expense of moderate multi-path transmission overhead only. Berman (2004) in the paper "Enhancing Data Security in Mobile Ad Hoc Networks via Multipath Routing and Directional Transmission" a cross-layer approach is studied to improve data security in Mobile Ad Hoc Networks (MANETs). A thorough evaluation shows that these mechanisms can also improve data availability. In addition, this study presents a security-oriented analysis of several important design details that are associated with multipath message exchange.

Papadimitratos (2006) in the paper "Secure Data Communication in Mobile Ad Hoc Networks" address the problem of secure and fault-tolerant communication in the presence of adversaries across a multihop wireless network with frequently changing topology. To effectively cope with arbitrary malicious disruption of data transmissions, they propose and evaluate the secure message transmission (SMT) protocol and its alternative, the secure single-path (SSP) protocol.

Rachedi (2006) in the paper "A Secure Architecture for Mobile Ad Hoc Networks" proposed a new architecture based on an efficient trust model and clustering algorithm in order to distribute a certification authority (CA) for ensuring the distribution of certificates in each cluster. Chasaki (2008) in the paper "Topology Reconstruction via Path Recording in Secure MANET" provides a discussion of different path recording mechanisms. They evaluate their performance in terms of packet overhead and reconstruction complexity. Luis et al. (2008) in the paper "Securing the communication in Private Heterogeneous Mobile Adhoc Networks" proposed the method a pair-wise key based scheme for forming secured private clusters in mobile ADHOC networks. The solution tackles the problem of node authentication combined with traffic encryption in relatively small ADHOC networks using proactive neighbour discovery and authentication. M.A.Matin et al (2009) in the paper "Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN" proposed a method on symmetric encryption technique with AES algorithm in MANET and WLAN. Symmetric encryption is faster and requires less computational processing time. The increase in key size as well as block size, the security gets enhanced and linear cryptanalysis and differential cryptanalysis require more time to break the proposed cipher here. Hongbo Zhou et al (2009) in the paper "Secure auto configuration and Public key Distribution for Mobile Ad-hoc Networks" proposed a method of auto configuration which is a method to achieve uniqueness of address allocation with the help of IP address for each node. Liebeherr (2009) in the paper "An Overlay Approach to Data Security in Ad-Hoc Networks" shows that overlay networks can provide forward and backward secrecy for application data in an ADHOC network. Mare.S.F. et al. (2011) in the paper "Secret data communication system using stenography, AES and RSA" proposed a method that uses AES, RSA for securing sensitive data that assures integrity, authenticity and security. Srivastava (2012) in the paper "Secure Data Transmission in MANET Routing Protocol" focussed on achieving the routing and secure information exchange ensuring confidentiality, integrity and authentication of data exchange in a more suitable and secured way.

III. CONCLUSION & FUTURE SCOPE

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism. These factors have changed the battle field situation for the MANETs against the security threats. This study has considered the hybrid system using PGP & DES encryption algorithm as a means of enhancing data security with respect to outsider attacks.

REFERENCES

[1] Network Centric Warfare, Department of Defence, Washington, DC, Jul. 2001, report to Congress.
[2] Global Information Grid Architectural Vision, Department of Defence, Washington, DC, Jun. 2007.
[3] Renu Dalal, Yudhvir Singh and Manju Khar, "A Review on Key Management Schemes in MANET" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012.
[4] Panagiotis Papadimitratos, Zygmunt J. Haas., "Secure message transmission in mobile ad hoc networks."
[5] Jorg Liebeherr and Guangyu Dong, "An Overlay Approach to Data Security in Ad-Hoc Networks"
[6] Danai Chasaki, Y. Sinan Hanay and Tilman Wolf, "Topology Reconstruction via Path Recording in Secure MANET" 978-1-4244-2677-5/08/$25.00 _c 2008 IEEE.
[7] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Transmission in Mobile Ad Hoc Networks" ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003.
[8] Abderrezak Rachedi and Abderrahim Benslimane, "A Secure Architecture for Mobile Ad Hoc Networks" International Conference on Mobile Ad-hoc and Sensor Networks (MSN'2006), Hong Kong : China (2006) DOI : 10.1007/11943952_36.
[9] VLADIMIR BERMAN, "Enhancing Data Security in Mobile Ad Hoc Networks via Multipath Routing and Directional Transmission".
[10] Panagiotis Papadimitratos and Zygmunt J. Haas,

"Secure Data Communication in Mobile Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[11] Kartik Kumar Srivastava, Avinash Tripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" IJCTA , Int.J.Computer Technology & Applications,Vol 3 (6), 1915-1921 Nov-Dec 2012. Available online@www.ijcta.com

[12] Danai Chasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in Secure MANET".

[13] Vineetha S. H. and Shebin Kurian, "Performance Analysis of Cluster Based Secure Multicast Key Management in MANET" **I**nternational **J**ournal of **C**omputer **S**cience and **T**elecommunications [Volume 4, Issue 4, April 2013].

[14] Ranjeet Singh, and Prof. Harwant Singh Arri, "COMPARISON OF AAMRP AND IODMRP USING SBPGP" International Journal of Computer Science and Management Research, Vol 2 Issue 3 March 2013.ISSN 2278-733X.

[15] Merin Francis, M. Sangeetha, and Dr. 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, Volume 3, Issue 1, January 2013, ISSN: 2277 128X.

