International Journal of Wireless Networks and Communications.
ISSN 0975-6507 Volume 4, Number 1 (2012), pp. 1-10

http://www.irphouse.com

SBPGP Security based Model in Large Scale Manets

Jashanvir Kaur and Er. Sukhwinder Singh Sran

Yadavindra College of Engineering,
Talwandi Sabo, Bathinda, Punjab, India
E-mail id: jashan_vir@yahoo.co.in, sukhwinder.sran@gmail.com

Abstract

The requirement of today is to provide secure and reliable communication of MANETs. So there is need for Key management and authentication are the central aspects of providing security in MANETs so these should not be weak. Security has no much issue for a small network but when number of mobile nodes is large and flexible then security must be provided at a large extent. PKI, PGP and SPGP plays the vital role in terms of the security. It is easy to manage the security of a fixed network but for a mobile and dynamically changing network it is very difficult. As malicious node can easily attack. Thus in this current paper we are focus on the security with Public key infrastructures and its various types that can help to maintain the security in the Mobile adhoc network.

Key terns: MANETS, PKI, PGP, SPGP

Introduction

An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multi-hop paths through the network to any other node [11]. This idea of Mobile ad hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly.

Certification

Public key certificate is the prerequisite for proving identity authentication between mobile ad hoc networks (MANET) nodes. However, for MANET's dynamic topologies and infrastructure-less, that bring the challengers for public key verification, similarly in hierarchical Public Key Infrastructure (PKI) in MANET [3]. The results in terms of certificate convergence time. This model needs *more specific protocol for formal* verification and analysis.

MANET is riddled by issues like unreliability of wireless media, uncertain connectivity, host mobility and lack of infrastructure [9]. However, perhaps, a most important aspect of such networks is the problem of security. The computational load and complexity involved in this environment are strongly subject to the dynamic nature of network topology, especially the restriction by the node's available resources. Therefore, key management and authentication are a central aspect for security in MANET and thus they should not be weak. The given model is only for small scale networks using PGP Technique but model is not sufficient for scalable network

In Dynamic networks protocols are used like Dynamic Source Routing (DSR), Ad Hoc On demand distance Vector Routing (AODV). The performance of protocols should be analyzed in terms performance matrices [7]. The poor performances of DSR are mainly attributed to aggressive use of caching, and lack of any mechanism to expire stale routes or determine the freshness of routes when multiple choices are available. Also AODV is not so effective for lower loads.

PKI is a new security technology, its role is to provide information security services, can use it to ensure that the network information security [14]. This article describes the theoretical basis of PKI and related technologies and concepts, analysis and comparison of PKI-based trust model: hierarchical trust model, peer trust model, network trust model, hybrid trust model. Analyzes the current PKI trust management and related lack of trust management system, given the open network environment, trust management system should have features.

Certificate-based cryptography and ID-based cryptography have been designed under different theoretical backgrounds and they have their own advantages and drawbacks, but there have been few works which try to provide. a unique private key issuing protocol in the *singleauthority multiple-observer (SAMO)* model which can reduce the user authentication load a lot, but these schemes are subject to several attacks due to the lack of verifiable authentication of protocol messages In this paper we show that these two problems can be solved by combining certificate-based and ID-based cryptography. In the proposed scheme certificate is issued to user for user-chosen public key and ID-based private key is issued to user through a private key issuing protocol. In the private key issuing protocol user is authenticated using the certificate and protocol messages are blinded using the certified public key of the user, thus the private key issuing protocol becomes private and also verifiable, which solves the authentication problem of [22]. We further present the concept of *unified public key infrastructure (UPKI)* in which both certificate-based and ID-based cryptosystems are provided to users in a single framework. We also show that if interactions between end users are mainly executed using ID-based cryptography,

then end users don't need to manage other end users' certificates, which is a great efficiency gain than traditional PKI.

An ad hoc mobile network (MANET) is a collection of wireless mobile hosts that form a temporary network without the aid of any centralized administration or support. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may be multiple hops away from each other[30]. With those network Characteristics, security has become a primary concern for researchers to meet scientific challenges to market opportunities in term of confidentiality, authentication, integrity, availability, access control, and non-repudiation. In the same way and as a powerful tool in achieving security, the Key Management becomes a corner stone in MANET security by proposing an appropriate secure schema for handling cryptographic keying materials. The Key Management scope includes key generation, key distribution, and key maintenance. In this paper, we aim to evaluate and to present a recent overview on different research works on Key Management in MANETs.

Security in Ad Hoc Networks

There are a number of proposed solutions for security authentication and key management in MANET. Proposed authentication architecture for MANET, describing the formats of messages, together with protocols which achieve authentication as in the architecture can accommodate different authentication schemes. One quite useful approach to the problem comprises PGP-based schemes.

PGP-Based Solutions

The 'Public Key Infrastructure' (PKI) is the most scaleable form of key management. Several different PKI techniques exist, such as SPKI, PGP and X.509. Various forms of these PKI techniques have been proposed for use in ad-hoc networks. Ref. [9] on security architecture proposes the use of a group-oriented PKI for large group formation. The leader of the group acts as a 'Certificate Authority' (*CA*), which issues group membership certificates. These are said to be SPKI-style certificates. They certify that the public key in the certificate belongs to a group member. However, this is not useful for two-party communications or non group-oriented tasks. on self-organized public key certificate management works like PGP [9], which allows users to create, store, distribute, and revoke their public keys without the help of any trusted authority or fixed server. This system does not assign specific missions to a node or subset of nodes (i.e. all the nodes have the same role). In this system, like in, users' public and private keys are created by the users themselves. It is assumed that each honest user owns a single mobile node. Hence the same identifier is used for the user and the other node (i.e. both being denoted by u). Unlike in PGP, where certificates are mainly stored in centralized certificate repositories, certificates in proposed system are stored and distributed by the nodes in a fully self-organized manner. Each certificate is issued with a limited validity period and therefore contains its issuing and expiration times. Before a certificate expires, its issuer issues an updated version of the same certificate, which contains an extended expiration time. This updated

version is called the certificate update. Each node periodically issues certificate updates, as long as its owner considers that the user-key bindings contained in these certificates are correct. In this system, key authentication is performed via chains of public-key certificates in the following way: When a user *u* wants to obtain the public key of another user *v*, he / she acquires a chain of valid public-key certificates such that

1. The first certificate of the chain can be directly verified by *u*, by using a public key that *u* holds and trusts (e.g. her own public key).
2. Each remaining certificate can be verified using the public key contained in the previous certificate of the chain.
3. The last certificate contains the public key of the target user *v*.

In this system, the certificate revocation is an important mechanism. It enables two types of certificate revocation: explicit and implicit. The issuer explicitly revokes a certificate by issuing a revocation statement and by sending it to the nodes which stored the certificate in question. The implicit revocation relies on the expiration time contained in the certificates. Every certificate whose expiration time passes is implicitly revoked; this second mechanism is straightforward, but requires some loose time synchronization of the nodes.

The quest for security in MANET led a PGP type PKI. In PGP, any node can issue a certificate and as such it allows a completely distributed architecture, apart from the central repository, which holds these certificates. It proposes a scheme to avoid the need for a central repository of certificates in the PGP system. This scheme involves each node keeping mini-repositories, which hold all the certificates the node issues and all the certificates issued on it. When nodes *A* and *B* meet, they merge their mini-repositories. The repositories are constructed according to the 'Shortcut Hunter algorithm' . This algorithm constructs repositories such that two nodes merging repositories have a high probability of finding a chain of certificates between them if one exists. This scheme is useful in a civilian environment where delegation of trust through a number of nodes is acceptable. Let the notation $A \rightarrow B$ mean that *A* trusts *B*. Then what the implications $A \rightarrow B$, $B \rightarrow C$, $C \rightarrow D$ and $D \rightarrow E$ signify is that *A* chooses to trust *E* i.e. $A \rightarrow E$. An alternative approach is to use a Certificate Authority (*CA*) to issue certificates. A *CA* is a third party trusted by all in the system, which effectively eliminates the need for a repository of certificates. Rather than finding a certificate linking $A \rightarrow B \rightarrow C \rightarrow D \rightarrow E$, one simply recovers the certificate $A \rightarrow E$. As such, the *CA* can be seen as a one-hop shortcut through the web of trust. The problem with this is the *CA* must be trusted by all and becomes a single point of failure in the event of an attack..

The SB-Trust Model

In PGP's "web-of-trust" model [9], each entity manages its own trust based on direct recommendation and seeks to further quantify the notions of trust and recommendation it uses a seniority-based (SB) trust model which is as follows. Trust management and maintenance are distributed in both space (*k*) and time (*T*) domains in the SB-model. Thus SB-model describes a seniors-securing approach to node

authentication in MANET. In other words, the parameter *T* characterizes the time-varying feature of a trust relationship, while *k* signifies the number of senior nodes required to work as *CA.* An entity is trusted if any *k* trusted available senior entities claim so within a certain time period *T*. Once a node is trusted by its senior group, it is globally accepted as a trusted node. Otherwise, if the seniors distrusted an entity then it is regarded as untrustworthy in the entire network. If a node cannot find *k* senior nodes in certain network, it may roam to meet more nodes or wait for new senior nodes to move in.

Construction of SB-PGP Model

In this work, we apply the SB-model for issuing PGP type certificate. Let us consider a MANET, to be established, for instance, in a conference where people having mobile nodes communicate with one another having insecure wireless channel. I assume N mobile nodes, and N may be dynamically changing as mobile nodes join, leave, or fail over time. Among them, some of the nodes that joined in the beginning are considered as senior nodes and later joining nodes are considered junior nodes but the size of senior nodes group may increase dynamically and sequentially according to the size of network. Besides, N is constrained if there may be a large device population otherwise not.

Specifically, for the model construction, we make the following assumptions:

- Each node has a unique nonzero ID and a mechanism to discover available senior member nodes of the network.
- Communication with senior nodes is more reliable compared with junior nodes of the networks.
- Mobility is centralized by a maximum node moving speed Smax .
- Each senior node is equipped with some local detection mechanism to identify Misbehaving nodes among its surrounding nodes, e.g. those proposed in [6, 1].
- All nodes are maintaining the seniority table like routing table.

Two nodes having off line certificate holder are used to centralize. Thus SB-PGP model describes a seniors-securing approach for issuance of PGP type certificate to a node & authentication in MANET. in which two or more (up to k) senior node are collectively sign a PGP type certificate and issue it to a newly incoming node after satisfying its information in T time. In other words, the parameter T characterizes the time-varying feature of a trust relationship, while k signifies the number of senior nodes required to sign on PGP type certificate or to work as CA. An entity is trusted if any k trusted available senior entities then it is globally accepted as a trusted node, Otherwise, untrustworthy for the entire network.

The architecture of the model resulting from these assumptions is given in the following section.

Architecture of SB-PGP Network

Consider a SB-trust model and introduce the PGP type certification design, which is

based on the de facto standard RSA. Now what is the structure of group of senior nodes working as CA. To see this, consider a network environment which does not follow a hierarchical or centralized control and fixed infrastructure and all member of the network are equivalent in terms of status. In this model functionality of the CA is performed by two or more senior most nodes of the network. These senior nodes collectively sign on the certificate of a new node, after satisfying themselves about its information. PGP type certificate is signed by more then one node. The size of CA nodes increases dynamically. Initially we divide our ad-hoc networks nodes in two groups, senior group SN and junior group JN. The size of senior group increases dynamically. Let

$$SN = \text{ceiling } (N \times M\ \%) + 1 \quad (1a)$$

Where SN = (set of senior nodes in senior group) N = (total number of nodes in ad-hoc network) (1b)

SCA = (set of nodes required for CA functionality)

M = (variable %).

Notice that M can change according to security level required in the networks. If M increases then the size of the senior group increases and availability of the networks also increases. However, security of the network decreases, because if the seniority number of a node is lower down, then its confidence level is also down.

$$SCA = \text{ceiling } (SN \times K\%) + 1 \quad (2a)$$

Where

SCA = (umber of senior most nodes required in the network for CA)

SN = (senior-most nodes)

K = (Variable %) (2b)

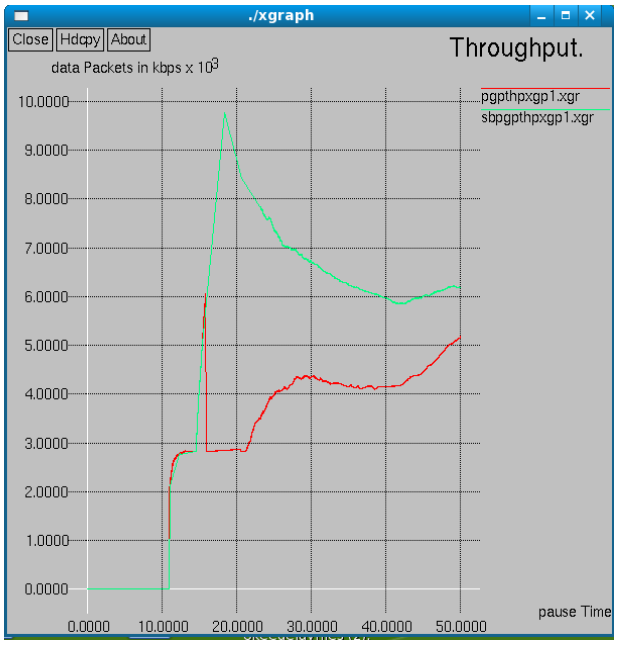
K : Depends on M. K can change according to security level required in the networks. If K increases then the number of nodes require for CA also increases and security of the network increases but availability of the CA of network decreases. Here SCA is number of senior most nodes require for CA to sign on the certificate for new reliable node. The signature procedure by each senior node of CA is done sequentially[9].

Again, notice that the junior group consideration involves a dynamic topology, which is proportional to the network size and senior group size. Consequently, the size of junior group (JN) will grow with the difference of growth in total number of nodes (N) of the network being considered and the growth in size of senior group (SN), which results in the following equation

$$JN = N - SN\ .$$

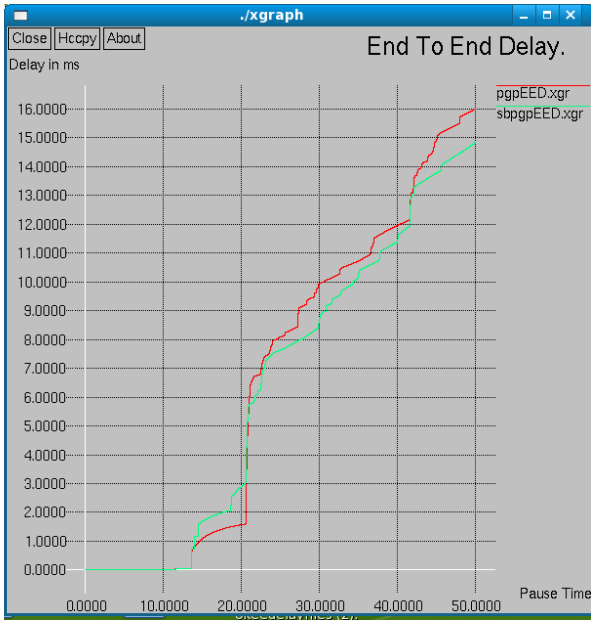
Throughput or network throughput: The average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. The system throughput or aggregate throughput is the

sum of the data rates that are delivered to all terminals in a network. The throughput data packet is higher in SBPGP as compared to PGP for the AODV protocol



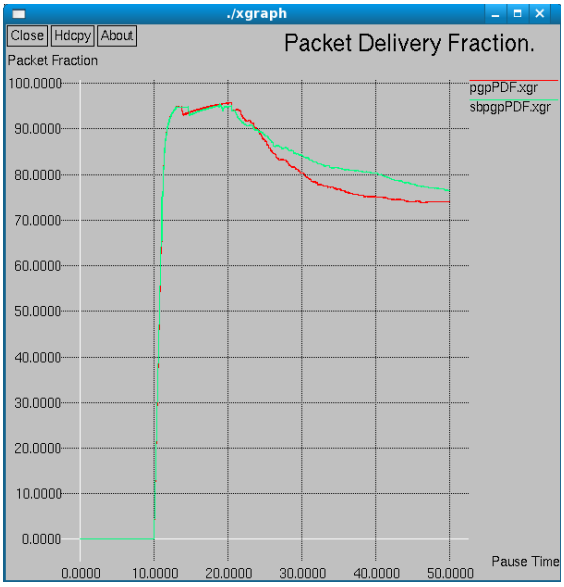
3 Average end-to-end delay of data packets

This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. The average end-to-end delay of packet delivery is higher in PGP as compared to SBPGP. For the AODV protocol.



Packet Delivery Fraction

The ratio of the data packets delivered to the destinations to those generated by the CBR sources. The delivery fraction is higher in SBPGP as compared to PGP. For the AODV protocol



Conclusion

In this current thesis work we have described the design of secure techniques namely PGP and SBPGP with AODV protocol. It has been observed from the previous paper that SBPGP is giving the better security as compared to the other techniques of PKI model. Current study is performed for comparison analysis for SBPGP model with PGP security models. From the above graph results and averaging it is found that SBPGP is giving better results and gives better security.

Future Scope

In future these techniques may be implemented with multicast routing protocols such as the On-demand Multicast Routing Protocol (ODMRP). And result for the different performance matrices be scrutinize.

References

[1] Kimaya Sanzgiri, Daniel LaFlamme and Bridget Dahill, “Authenticated Routing for Ad hoc Networks” , Refinements and extensions to IEEE ICNP 2002.

[2] Svein Johan Knapskog, "New Cryptographic Primitives (Plenary Lecture)", 7th Computer Information System and Industrial Management Applications, IEEE 2008.
[3] Yue Ai and Fuwen Pang, "Improved PKI Solution for Mobile Ad Hoc Networks", IEEE 2010.
[4] Venkatesan Balakrishnan and Vijay Varadharajan, " Designing Secure Wireless Mobile Ad hoc Networks", 19th International Conference on Advanced Information Networking and Applications, IEEE 2005.
[5] G Varaprasad and P. Venkataram, "The Analysis of Secure Routing in Mobile Ad Hoc Network", International Conference on Computational Intelligence and Multimedia Applications, IEEE 2007.
[6] Nilesh P Bobade and Nitiket N Mhala, " Performance Evaluation of Adhoc On Demand Distance Vector in Manets with varying Network size using NS-2 Simulation", International Journal on Computer Science and Engineering (IJCSE) Volume 02 , August, 2010.
[7] Geetha Jayakumar and Gopinath Ganapathy, "Performance Comparison of Mobile Ad-hoc Network Routing Protocol", International Journal of Computer Science and Network Security (IJCSNS), Volume 07, November 2007.
[8] Kamarudin Shafinah and Mohammad Mohd Ikram, "File Security based on Pretty Good Rrivacy (PGP) Concept", www.ccsenet.org/cis, Computer and Information Science, Volume 04, July 2011.
[9] Maqsood Razi, Jawaid Quamar, "A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET" IEEE 2008.
[10] Antonio Vincenzo Taddeo, Alberto Ferrante, "A Security Service Protocol for MANETs", IEEE 2009.
[11] Q. Wang and W.C. Wong, "A Robust Routing Protocol for Wireless Mobile Adhoc Networks", IEEE 2002.
[12] Asad Amir Pirzada, Amitava Datta and Chris Mcdonald, "Trustworthy Routing with the AODV Protocol", IEEE 2004.
[13] Manali J Dubal, Mahesh T R and Pinaki A Ghosh, "Design of New Security Algorithm, Using Hybrid Cryptography Architecture", IEEE 2011.
[14] Hou Liping and Shi Lei, "Research on Trust Model of PKI", 4th International Conference on Intelligent Computation Technology and Automation, IEEE 2011.
[15] Jiang Haowei and Tan Yubo, "Research in P2P-PKI Trust Model", IEEE 2010
[16] Dongxia Li and Xinana Fu, "A Revised AODV Routing Protocol based on the Relative Mobility of Nodes".
[17] Radia Perlman (Sun Microsystems), "An Overview of PKI Trust Models", IEEE Nov-Dec 1999.
[18] Hisashi Mohri, Ikuya Yasuda, Yoshiaki Takata and Hiroyuki Seki, "Certificate Chain Discovery in Web of Truist for Adhoc Networks"21st International Conference on Advanced Information Networking and Application Workshops (AINAW) , IEEE 2007.

[19] Ping Yi, Tianhao Tong, Ning Liu, Yue Wu and Jianqing Ma " Security in Wireless Mesh Networks: Challenges and Solutions" , Sixth International Conference on Infoirmation Technology: New Generations, IEEE 2009.
[20] JuCheng Yang, "Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System", International Conference on Management of e-Commerce and e-Government, IEEE 2010.
[21] Azzedine Boukerche, "A Simulation Based Study of On-Demand Routing Protocols for AD hoc Wireless Networks" IEEE 2001.
[22] Byoungcheon Lee, "Unified Public Key Infrastructure Supporting Both Certificate Based and ID-Based Cryptography", International Conference on Availability, Reliability and Security, IEEE 2010.
[23] Hao Yang, Haiiyun Luo and Fan Ye, "Security in Mobile Ad hoc Networks: Challenges and Solutions", IEEE Wireless Communication, February 2004.
[24] http://isi.edu/nsnam/ns/
[25] Hassen Redwan and Ki-Hyung Kim, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks", ESR Groups France, IEEE 2008.
[26] M. Markovic, "Data Protection Techniques, Cryptographic Protocols and PKI System in Modern Computer Networks", IEEE Explorer.
[27] WU Xing-hui and MING Xiu-jun, " Research of the Database Encryption Technique Based on Hybrid Cryptography", International Symposium on Computational Intelligence Design, IEEE 2010.
[28] NS-2. The ns manual (formally known as NS Documentation) Available at http:// www.isi.edu/nsnam/ns/doc.
[29] Sasan Adibi, Shervin Erfani and Hani Harbi, " Security Routing in MANETs-A Comparative Study", IEEE Explorer.