Sbpgp Security Model Using Iodmrp

Meenakshi Mehla[1], Himani Mann[2]
[1]C.S.E, Kurukshetra University,
JMIT(Radaur), Haryana, India
[2]C.S.E, Kurukshetra University,
Kurukshetra, Haryana,Pin-136118,India

Abstract
Today's world is mobile and using ad hoc network. Routing is the reactive on-demand philosophy where routes are established only when required.Security is one of the most important concepts in ad hoc networks. So different strategies for security are suggested. The study here proposes a theory in this paper based on PKI with IODMRP. The study should help in making protocols more robust against attacks and standardize parameters for security in routinsg protocols. PKI, PGP and SPGP plays the vital role in terms of security.It is easy to manage the security of a fixed network but for a mobile and dynamically changing network it is very cumbersome. 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.

Keywords: *IODMRP MANETS, PKI, PGP, SPGP*

1. Introduction

Mobile Ad-Hoc Networks are autonomous and self-configuring wireless systems. MANETs consist of mobile nodes that are free to move in and out of the network. These node can be mobile phone, system etc. Mobility affects the power indulgence of the nodes in a MANET and has great impact on its security. IODMRP is a more efficient multicast routing protocol It chooses partial forwarding nodes to relay packets, the number of which is decided by probabilistic forwarding algorithm. Security is provided by use of PKI,PGP and SBPGP.SBPGP has better performance than others. Security is main concern in Manets because nodes are mobile.

1.2Security threat

The two broad classes of network attacks are active attacks and passive attacks.
Passive Attack**:** An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described as

- **Eavesdropping:** The attacker checks message contents on transmission line.
- **Traffic analysis:** The attacker, in a more subtle way, gains intelligence by monitor the transmissions for

patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

Active Attack: in this attack an unauthorized person modifies the message contents,files,etc. such type of attacks are easily detectable but can't be prevented.Active attacks may take the form of one of four types masquerading, replay, message modification, and denial-of-service (DoS). These attacks are summarized as:

- **Masquerading:** The attacker imitate an authorized user and thereby gains certain unauthorized rights
- **Message modification:** The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- **Denial-of-service:** The attacker prevents or prohibits the normal use or management of communications facilities.

1.3 Related Work

Many security models have been used PKI,PGP . every model gives different types of performance matrices. Maqsood Razi and Jawaid Quamar proposes paper on hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET. Kamal Kumar Chauhan1, Amit Kumar Singh Sanger2, Virendra Singh Kushwah3 proposes Securing On-Demand Source Routing in MANETs.They conclude a protocol to secure on demand source routing in MANETs that fulfills the security requirements. Our protocol uses one way hash function to maintain the integrity of message. Therefore, deletion of a node from or any kind of modification in route control packetcan be detected. Using Public Key Cryptography (PKC),nodes can negotiate the session key for secure communication that fulfills the requirement of confidentiality. Source, destination and intermediate nodes in route list authenticate others

nodes by verifying signature. Security analysis results show that protocol provides the security against many attacks such as reply attack, rushing attack, IP spoofing and man in the middle attack. Our protocol is based on Public Key Cryptography. Asymmetrical algorithms require more calculation than the symmetrical algorithms. Therefore, it consumes much battery power than protocols based on symmetric algorithms.

2.Proposed Technique

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

2.1 PGP-Based Solutions

The 'Public Key Infrastructure' (PKI) is the most scalable 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..

2.2 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.

2.3 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.

2.4 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 = ceiling (N × M %) + 1 (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 = ceiling (SN × K%) + 1 (2a)

Where

SCA = (number 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

3. METHOLOGY

3.1 Simulation Environment

Simulations are done to compare these routing protocols. Simulator ns-2 is used for performance comparison. The network simulator ns-2 developed by the VINT research group at University of California at Berkeley in 1995 . The network simulator NS2 is a discrete event network simulation. Ns is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

NS2 is used to simulate the proposed algorithm. It work on network layer and inform about link breakage. The implementation of the protocol has been done using C++ language in the backend and TCL language in the frontend. TCL(Tool Command Language) is compatible with C++ programming language.
Interpretation is based upon two files trace files and nam files are to be generated. Network Animator (.nam) file, records all the visual events that happened during the simulation. Trace files (.tr), records the entire network event that occur during the simulation. And file is post analyzed with the help of awk scripts..

Table 2 : Simulation Parameter

Parameter	***value***
Simulation Time	50 Sec
No. of Nodes	50
Traffic Type	CBR
Pause Time	10 Sec
Maximum X-Y coordinate value	1000 M
Packet Size	512 byte
MAC Protocol	802.11
Mobility Model	Random Waypoint
Routing Protocol	IODMRP
Observation Parameters	EED, Throughput, PDF

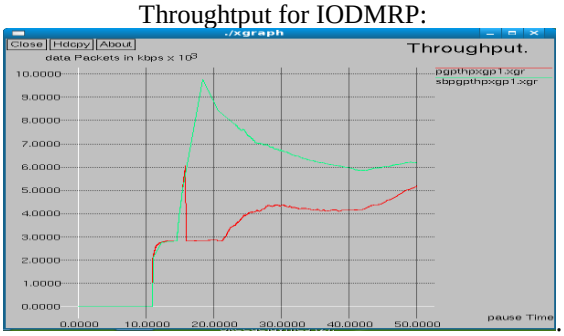
3.2 Performance Metrics:
The estimation of performance of AODV, OLSR and TORA is done on the basis of following Performance metrics:

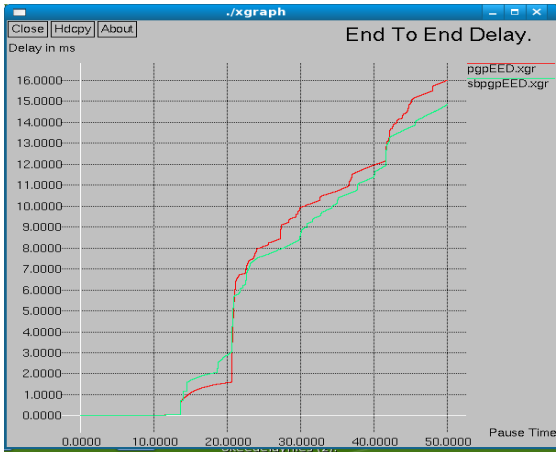
- **Packet Delivery Ratio:** It is the ratio of the packets received by destination to those generated by the sources. CBR traffic type is used by source. It specifies the packet loss rate, which limits the maximum throughput of the network. The routing protocol which have better PDR, the more complete and correct. This reflects the usefulness of the protocol. And provide good performance.

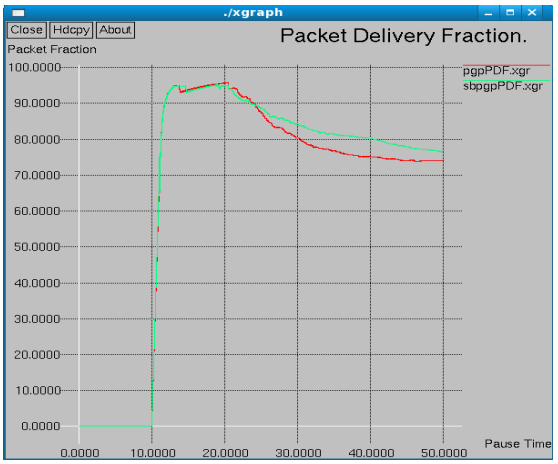
  Packet Delivery Ratio = (Received Packets/Sent Packets)
- **End to End Delay:** Average end-to-end delay is the average time it taken by the packet to reach to destination in seconds.
- **Throughput:** No. of packet passing through the network in a unit of time. It is measure in kbps.

4. Results

Throughtput for IODMRP:







5. Conclusion

In this current thesis work we have described the design of secure techniques namely PGP and SBPGP with IODMRP 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.

6 Acknowledgement

First and foremost, I would like to express my sincere gratitude to my guide Mrs. Meenakshi Mehla, Assistant Professor, Computer Science and Engineering Department for immense help, guidance, stimulating suggestions, and encouragement all the time with this thesis work. This work would have not been possible without her support. She always provided a motivating and enthusiastic atmosphere to work with; it was a great pleasure to do this thesis under her supervision.
Most importantly, I would like to thank my parents and the almighty for showing me the right direction, to help me stay calm in the oddest of times and keep moving at times when there was no hope.
Himani Mann

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.