Performance Evaluation of AODV and DSDV under Seniority Based Pretty Good Privacy Model (SBPGP)

Nidh Mittal , Janish

Abstract: The routing protocols are to maximize network throughput, to maximize network lifetime, to maximize energy efficiency and to minimize delays. The network throughput is measured by packet delivery ratio and energy contribution is measured by routing overhead which is number or size of routing control packets. When the security model is applied they behave different. The effective of the overhead we have to analyze and study in the current research work. We are applying the current technique with DSDV and AODV routing protocol. This scheme can make most of the on demand protocols secure. The study should help in making protocols more robust against attacks and standardize parameters for security in routing protocols. 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.

Index terms: MANETS,PKI, PGP, SBPGP,AODV,DSDV

1 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.

2 SECURITY REQUIREMENTS

In any fixed or wireless network, the security is incorporated at three stages: prevention, detection and cure. Key parts of prevention stage are authentication and authorization. The authentication is associated with authenticating the participating node, message and any other meta-data like topology state, hop counts etc. Authorization is associated with recognition. Where detection is the ability to notice misbehavior carried out by a node in the network, the ability to take a corrective action after noticing misbehavior by a node is termed as cure.

Different possible attacks on ad hoc networks are eavesdropping, compromising node, distorting message, replaying message, failing to forward message, jamming signals etc. The central issues behind many of the possible attacks at any level of security stage are authentication,

- Nidhi Mittal, Faculty(ECE),Doon Valley Institue of Engg and Tech,Kurukshetra University,Karnal 132001,India. Email-mail2bansal@gmail.com.
- Janish, Mtech(ECE),Doon Valley Institue of Engg and Tech,Kurukshetra University, Karnal 132001,India. Email-nain.jenice@gmail.com.

confidentiality, integrity, non repudiation, trustworthiness and availability.

There are several proposals [7] available to solve these issues, but are not comprehensive in nature as they target specific threats separately. Therefore there is a strong need to have an efficient security regime which can take care of all the aspects of security.

3 SECURITY THREATS

The two broad classes of network attacks are active attacks and passive attacks.

3.1 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 monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a network topology between two workstations or tuning into transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station. analysis).
- **Traffic analysis:** The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

3.2 Active Attack: An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. 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 impersonates an authorized user and thereby gains certain unauthorized privileges.
- **Replay:** The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
- **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.

The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service.

Ad hoc networks face many problems due to which a consistent and secure network flow becomes challenging task. Some of the issues associated are given below.

1) Ad Hoc networks primarily being wireless have limited band-width in comparison to wired networks. Smaller packets are available to transfer data and it further constraints to use lesser number of bits for security purposes. It has been expected that this limitation will be eased with the advancement of hardware in future.

2) The participating nodes of an Ad Hoc networks usually are mobile devices which have limited capabilities in terms of processing power, memory size and battery backup. It makes the use of digital signature [4], as a security measure less suitable as digital signatures are computation intensive. The use of digital signatures may also consume considerable memory if digital signatures are appended by each node that forwards the packet to its destination. Furthermore a PKI [14] infrastructure is not practical in case of Ad Hoc networks. Other problem with use of digital signature is to maintain a certificate revocation list (CRL), in the absence of a central server. The solution to this problem can be achieved by using some light weight security arrangements only.

3) The use of hashing techniques although offer efficient security measures but have been used relatively less. Hashing technologies like MAC [4], HMAC [4], one way hash chains [8] etc have mostly been used for authenticating routing and message information. The effectiveness of hashing techniques depends on the way the collisions have been treated.

4 SECURE ROUTING

The routing protocols [1,2,3] with in ad hoc networks are more vulnerable to attacks as each device acts as a relay. Any tampering with the routing information can be compromise the whole network. An attacker can introduce rogue information with in routing information or replay old logged or stored information.

The aim is to protect any information or behavior that can update or cause a change to the routing tables on cooperating nodes involved in an ad hoc routing protocol. For completeness, timeliness and ordering are added to the list of desirable security properties that can eliminate or reduce the threat of attacks against routing protocols.

5 DESCRIPTION OF THE AD-HOC ROUTING PROTOCOLS

5.1 Destination-Sequenced Distance-Vector (DSDV)

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm is based on the idea of the classical Bellman-Ford Routing algorithm with certain improvements.

Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven.

The routing table updates can be sent in two ways: - a "full dump" or an incremental update. A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. If there is space in the incremental update packet then those entries may be included whose sequence number has changed. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps will be more frequent.

5.2 Ad Hoc On-Demand Distance Vector Routing (AODV)

AODV shares DSR’s on-demand characteristics in that it also discovers routes on an *as needed* basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers.

An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is *expired* if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs. Route error propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves.

6 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.

6.1 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.

6.2 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.

6.3 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 = (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 $JN = N - SN$.

7 METHOLOGY

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.

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	AODV, DSDV
Observation Parameters	EED, Throughput, Packet Delivery Ratio

8 PERFORMANCE METRICS:

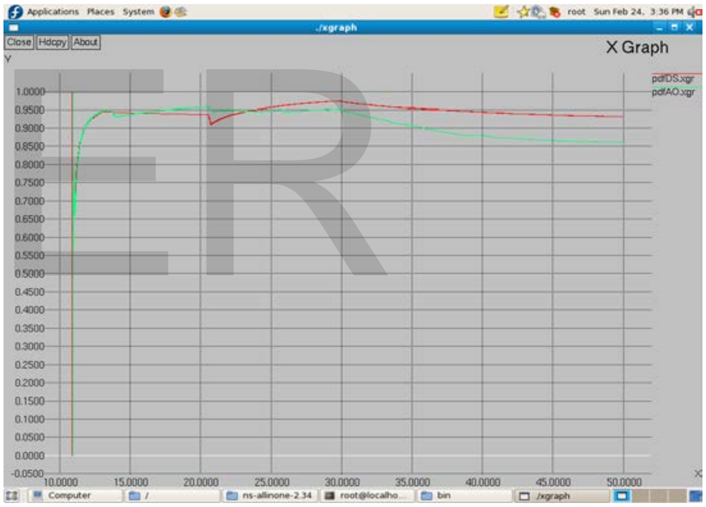
The estimation of performance of AODV, DSDV is done on the basis of following Performance metrics:

- **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.

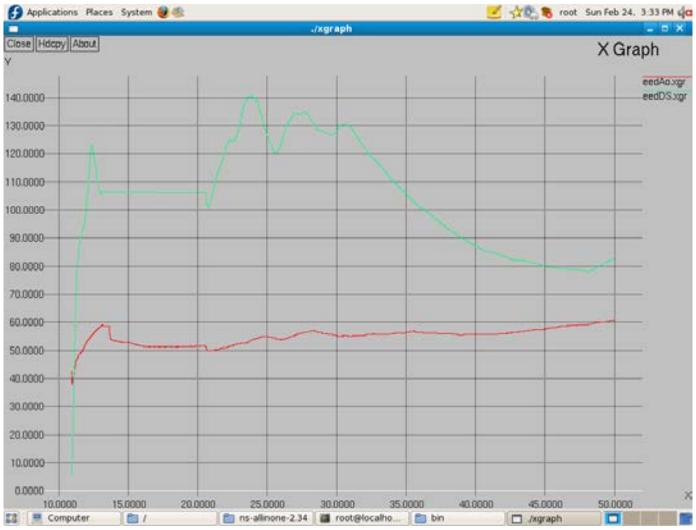
  Packet Delivery Ratio = (Received Packets/Sent Packets)
- **End to End Delay:** Average end-to-end delay is the average time it taken by the packet to reach to destination in seconds.
- **Throughput:** No. of packet passing through the network in a unit of time. It is measure in kbps.

9 RESULTS

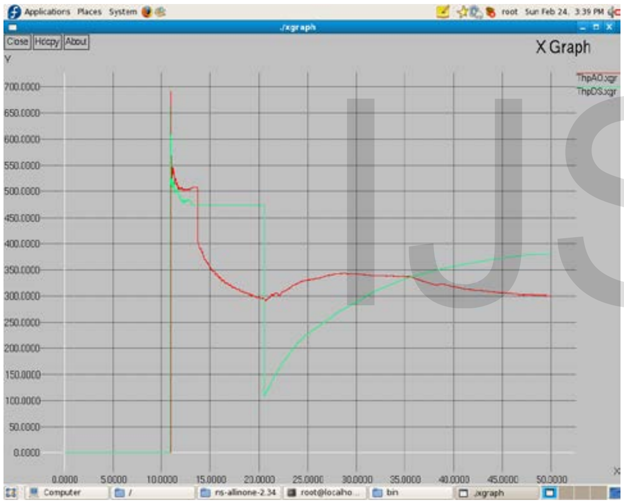
Packet delivery ratio for AODV and DSDV



End to End Delay for AODV and DSDV



Throughput for AODV and DSDV



10 CONCLUSION

It is checked that AODV is well behave during end to end delay and is throughput but delivery packet fraction is slow. In future these techniques may be implemented with multicast routing protocol and result for the different performance matrices be scrutinize .

REFERENCES:

[1] Kimaya Sanzgiri, Daniel LaFlamme and Bridget Dahill, “Authenticated Routing for Ad hoc Networks” `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.