International Journal of Research in Computer Engineering and Electronics. 1
VOl : 2 ISSUE :1 (Feb 2013)
ISSN 2319-376X

Design and Analysis of Secure Quality-Of-Service Routing in Mobile Ad Hoc Networks

Bharat Bhushan Naib[1], Dr. V.R. Singh[2]

Abstract— An ad hoc network is a collection of computers (nodes) that cooperate to forward packets for each other over a multihop wireless network. Users of such networks may wish to use demanding applications such as videoconferencing, Voice over IP, and streaming media when they are connected through an ad hoc network. Because overprovisioning, a common technique in wired networks, is often impractical in wireless networks for reasons such as power, cost, and government regulation, Quality of Service (QoS) routing is even more important in wireless networks than in wired networks. Though a number of QoS-routing protocols have been proposed for use in ad hoc networks, security of such protocols has not been considered. SQoS relies entirely on symmetric cryptography. Symmetric cryptographic primitives are three to four orders of magnitude faster (in computation time) than asymmetric cryptography. In this research paper, SQoS is simulated using NS-2 and the parameters used for simulation are throughput, packet-loss and end-to-end delay. SQoS helps in providing security and Quality of Service in MANET.

Index Terms— Simulations, security, Quality-of-Service, QoS routing, ad hoc networks, SQoS.

1 INTRODUCTION

1.1 Review Stage

An ad hoc network is a collection of computers (nodes) that cooperate to forward packets for each other over a multihop wireless network. The nodes in the network may move and radio propagation conditions may change at any time, creating a dynamic, rapidly changing network topology. An important application of ad hoc networking technology is to enable communication in environments in which there is no infrastructure, where the infrastructure has been destroyed, or when the infrastructure cannot be used due to issues such as cost and security. A substantial amount of research has been proposed in the field of ad hoc network routing, and mature protocols such as DSR, AODV, OLSR, and TBRPF have emerged from standards discussions in the Internet Engineering Task Force (IETF), the principle protocol standards development organization for the Internet. Users of ad hoc networks may wish to use demanding applications such as videoconferencing, Voice over IP, and streaming media when they are connected through an ad hoc network. Quality of Service (QoS) has been an important area of research in wired networks, as researchers have looked for solutions that provide acceptable levels of performance for these types of applications.

In wireless networks, QoS routing is even more important. That is, in wired networks, overprovisioning can often be used to reduce the need for sophisticated QoS techniques in all but the most demanding network applications.

- [1] Bharat Bhushan Naib is Research Scholar, Mewar University, Rajasthan. India.
- [2] Prof. (Dr.) V.R. Singh, Director, PDMCE, Bahadurgarh, Haryana.India.

However, in wireless networks, overprovisioning is often impossible or impractical, due to constraints on radio spectrum and power level, or because of interference or noise within the radio spectrum. As a result, using a QoS routing protocol to carefully choose routing paths with sufficient resources may be the only way to provide sufficient resources in wireless networks for many applications. Routing protocols for ad hoc networks can generally be divided into two categories.

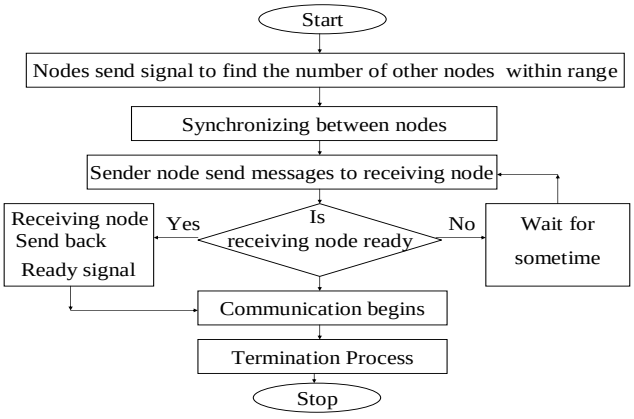

Figure 1: Working of a general Ad-Hoc Network

For dynamically mobile ad hoc networks, reactive or on demand routing protocols often outperform proactive or periodic ones, due to their ability to adjust the amount of network overhead created to track the mobility in the network affecting current communication . The rest of this paper is organized as follows: In Section 1, we present an overview of adhoc networks and SQoS. In Section 2, we describe QoS-Guided Route Discovery, in Section 3 we describe cryptographic mechanisms that are used in SQoS and in Section 4 we describe the basic

operation of DSR. In this paper, Section 5 indicates about existing problem. Section 6 gives implementation results and Section 7 gives the conclusion

2.QoS-Guided Route Discovery

In an on-demand ad hoc network routing protocol, such as DSR or AODV, a node (which we call the initiator) can find a route to a destination node (which we call the target) by performing a controlled flood of the network. In this Route Discovery procedure, the initiator transmits a ROUTE REQUEST packet, identifying the target to which the route is needed. Each node receiving the ROUTE REQUEST in general retransmits the REQUEST if it has not already forwarded a copy of it; when the target node receives the REQUEST, it returns a ROUTE REPLY to the initiator, listing the route taken by the REQUEST, rather than forwarding the REQUEST. Many optimizations have been defined for this basic Route Discovery scheme to reduce the frequency of performing Route Discovery and to limit the portion of the network over which the ROUTE REQUEST flood must be forwarded.

3. Cryptographic Mechanisms

We design SQoS, our secure QoS routing protocol, by building on existing security mechanisms. Specifically, SQoS builds on hash chains and MW-chains.

3.1 Hash Chains

One-way hash chains are a widely used cryptographic primitive. One of the first uses of one-way chains was in one-time password protocols. These chains are also used in other applications, such as efficient one-time signature algorithm. Coppersmith and Jakobsson present efficient mechanisms for storing and generating values of hash chains. We create a one-way chain by selecting the final value vn at random, and by repeatedly applying a one-way hash function H, such that vi = H[vi+1]. The last value generated in this way is called the anchor; generally, an authentic anchor is published to allow verification of hash chain elements.

3.2 The MW Chains Mechanism

In this section, we review the MW-chain mechanism, which provides instant authentication and low storage overhead. First, we describe the one-time signature, on which MW-chains are based. In a signature, a node chooses a private key K, and from that private key generates a verification key V. Given a message m, the node can use K to form a signature s such that a node with V can verify the signature; however, a node with V but not K cannot generate a signature. A one-time signature is a type of signature such that only one message m can be signed with a single key. For example, in the Merkle-Winternitz one-time signature, two signatures using the same key provide an attacker enough information to forge certain other signatures. The MW-chain is built on a certain type of one-time signature, which we call a chainable signature. In a chainable signature, a signature s on message m can be verified by comparing f (s,m) to verification key V, and any verification key can be used as a signature key. One such one-time signature is the Merkle-Winternitz signature.

4. Basic operation of DSR

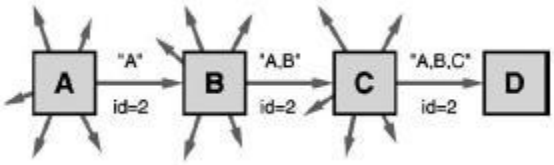

Figure.2 Example of DSR Route discovery

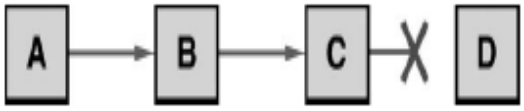

Figure .3 Example of DSR Route Maintenance

DSR is an entirely on-demand ad hoc network routing protocol composed of two parts: Route Discovery and Route Maintenance. In this section, we describe the basic form of Route Discovery and Route Maintenance in DSR. In DSR, when a node has a packet to send to some destination and does not currently have a route to that destination in its Route Cache, the node initiates Route Discovery to find a route; this node is known as the initiator of the Route Discovery, and the destination of the packet is known as the Discovery's target. The initiator transmits a ROUTE REQUEST packet as a local broadcast, specifying the target and a unique identifier from the initiator. Each node receiving the ROUTE REQUEST, if it has recently seen this request identifier from the initiator, discards the REQUEST. Otherwise, it appends its own node address to a list in the REQUEST and rebroadcasts the REQUEST. When the ROUTE REQUEST reaches its target node, the target sends a ROUTE REPLY back to the initiator of the REQUEST, including a copy of the accumulated list of addresses from the REQUEST. When the REPLY reaches the initiator of the REQUEST, it caches the new route in its Route Cache. Route Maintenance is the mechanism by which a node sending a packet along a specified route to some destination detects if that route has broken, for example because two nodes in it have moved too far apart. DSR is based on source routing: when sending a packet, the originator lists in the header of the packet the complete sequence of nodes through which the packet is to be forwarded.

5. Existing Problem:

Due to rapidly changing network topology and dynamic nature of MANET, security in MANET needs to be improved.

6. Implementation Results :

SQoS Results :

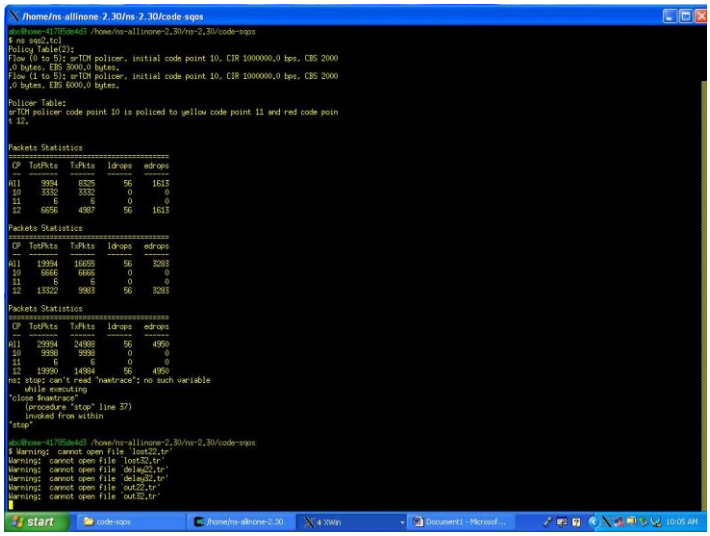

Figure 4.SQoS Packet Statistics-I

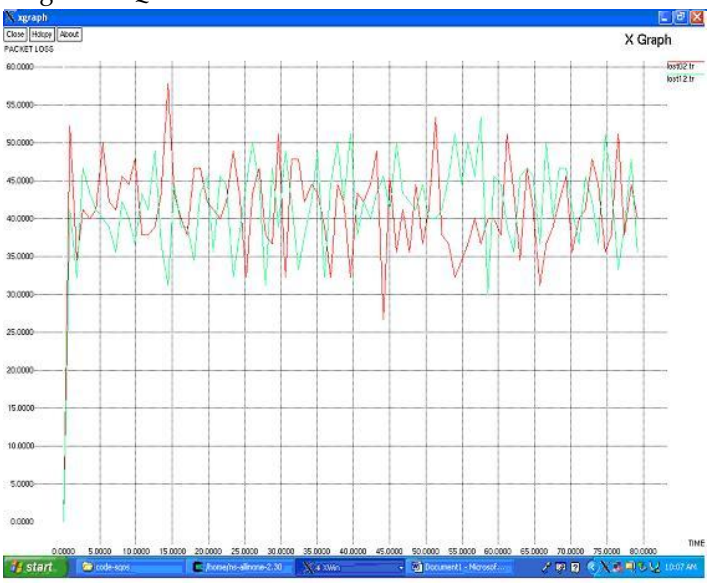

Figure 5.:Throughput

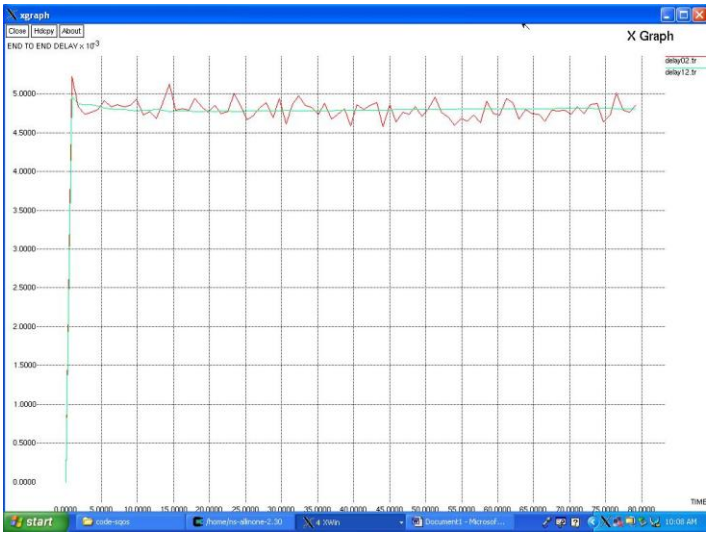

Figure 6.Packet Loss

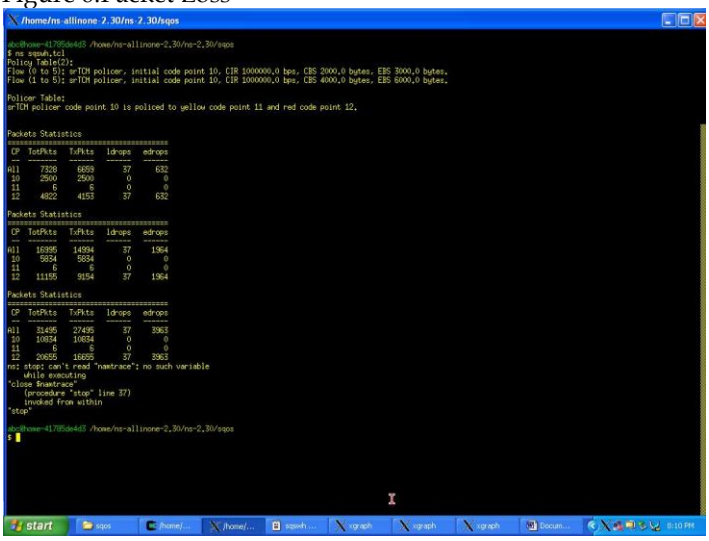

Figure 7: End-To-End Delay

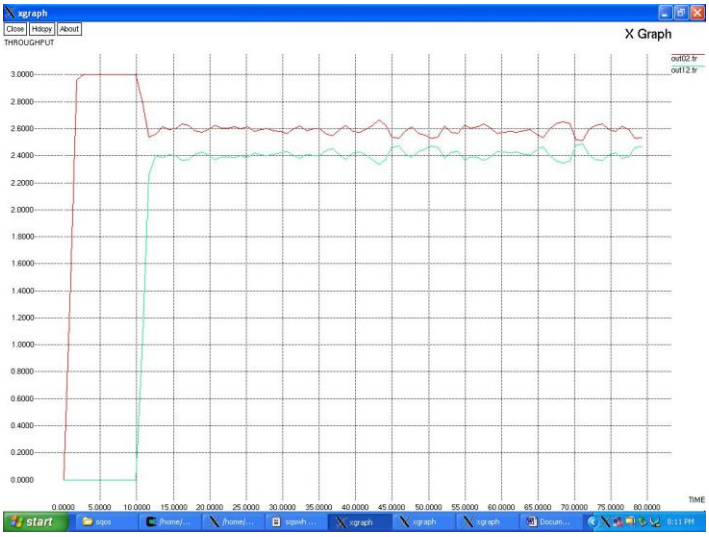

Figure 8.:SQoS Packet Statistics-II

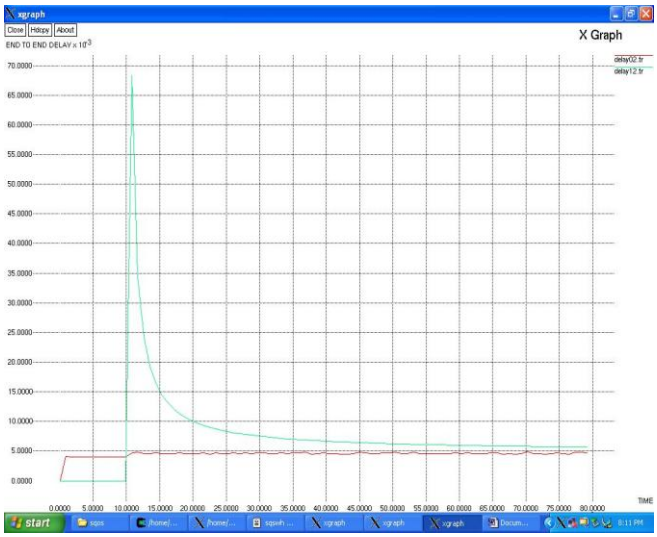

Figure 9.:Throughput

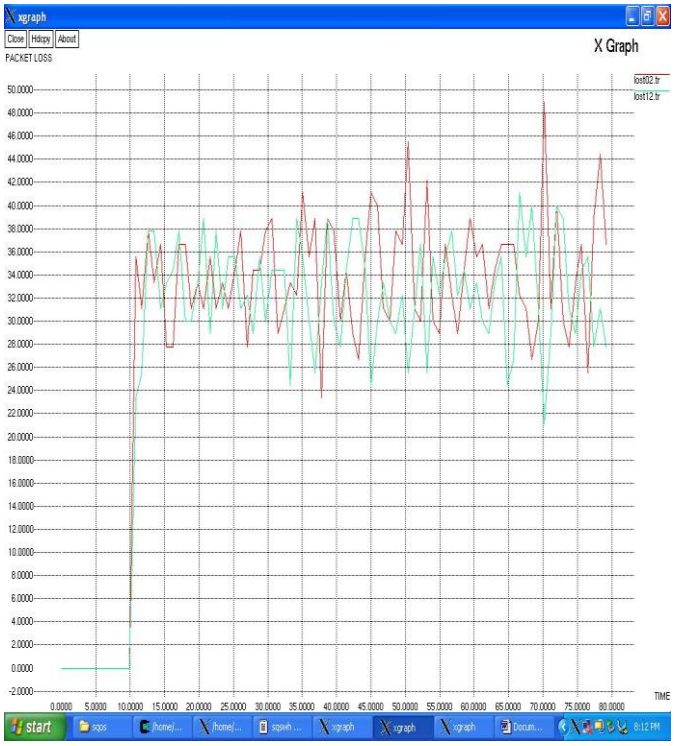

Figure 10.:Packet Loss

Result: Outcome Of NS-2 Simulation:

Table No.1: Shows Reduction in I Drops and E Drops

S. No.	I Drops (From packet Stats.-I)	I Drops (From packet Stats.-II)	E Drops (From packet Stats.-I)	E Drops (From packet Stats.-II)	Overall % Reduction in I Drops	Overall % Reduction in E Drops
1	56	37	4950	3963	33.9%	19.9%

7. Conclusion

In this research paper, SQoS protocol is used for MANET and is implemented on NS-2. The parameters used for simulation are throughput, end-to-end delay and packet-loss. In this re-

search paper, I Drops represent number of packets that are dropped due to link overflow and E Drops represent number of packets that are dropped due to RED early dropping. In this research paper, overall % reduction in I Drops is 33.9% and overall % reduction in E Drops is 19.9%.

References

[1]. Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, and Herbert Rubens. An On- Demand Secure Routing Protocol Resilient to Byzantine Failures. In ACM Workshop on Wireless Security (WiSe), September 2002.

[2]. Y. C. Hu and D. B. Johnson, "Securing quality-of-service route discovery in on- demand routing for Ad hoc networks", in Security of Ad Hoc and Sensor Networks 2004(SASN 2004), Washington, USA, Oct. 2004.

[3]. Y. C. Hu, A. Perrig, and D. B. Johnson, "Aridane: A secure on-demand routing protocol for Ad hoc networks", in Proceedings of the Eight Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp. 12-23, Sept. 2002.

[4]. Bob Braden, David Clark, and Scott Shenker. Integrated Services in the Internet Architecture: an Overview. RFC 1633, June 1994.

[5]. Josh Broch, David B. Johnson, and David A. Maltz. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. Internet-Draft, draft-ietf-manet-dsr-03. txt, October 1999. Work in progress. Available from http://www.monarch.cs.rice.edu/internet-drafts/ draft-ietf-manet-dsr-03.txt.

[6]. R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: an Overview," in RFC 1633, June 1994, http://www.ietf.org/rfc/rfc1633.txt.

[7]. S. Blake, D. Black, and M. Carlson, "An Architecture for Differentiated Service," in RFC 2475, December 1998, http://www.ietf.org/rfc/rfc2475.txt.

[8]. H.Xiao, W. K. G. Seahand, A. Lo, K. C. Chua, " A Flexible Quality Of Service Model for Mobile Ad-Hoc Networks," in proc. Of IEEE Vehicular Technology Conf. (VTC2000), Tokyo, Japan, May 2000, pp.445-449.