Int. J. Advanced Networking and Applications
Volume: 03, Issue: 04, Pages:1253-1260 (2012)

Improving Quality of Service Through Secured Routing In Mobile Ad Hoc Networks

Ananda Krishna B [1] , R.Ramesh[2]
[1]Professor, Department of ECE, Gudlavalleru Engineering College, Krishna Dt.AP,
Email: anand_bk@rediffmail.com
[2]Assistant Professor Selection Grade, Department of ECE, SRM University, Chennai,
Email: ramesh7373@gmail.com

----------ABSTRACT----------

Due to the high flexibility, mobility and low cost features, wireless ad hoc networks are widely used. A particularly challenging problem is how to feasibly detect and defend the major attacks against routing protocols of such networks that have susceptible links and dynamic topology. Most of the existing secure routing protocols for ad hoc networks either avoid the most challenging internal attacks such as Byzantine behaviors, or have often produced inefficient security mechanisms. In this paper, we propose the mechanism for securing the QoS route and to increase the probability of success in finding QoS feasible paths. Providing both security and QoS routing in MANET is the major challenge for this technology. Hence, we have addressed the QoS metrics, issue of security and its effectiveness. The performance of the proposed security model with QoS using GloMosim is studied and compared with and without QoS. From the results we observe that the overall network performance is improved with QoS.

KEY WORDS: Security, MANETs (Mobile Ad hoc Networks), QoS (Quality of Service), Routing, Authentication

Date of Submission: Date Revised: Date of Acceptance:

1. INTRODUCTION

In MANETs, node mobility often results in frequent topology changes, which presents a significant challenge when designing QoS routing protocols. It is unreachable for high node mobility to satisfy QoS requirements. Consequently, it is required that the network be combinatorially stable in order to achieve QoS support [1]. QoS support of MANETs requires availability of network state. However, due to mobility and constant topology changes, the cost of maintenance of the network state is expensive especially in large networks. In [2] the *imprecise network state model* is introduced. It provides a cost-effective method for providing QoS support based on imprecise network information. The majority of QoS routing protocols are reservation-based. Probe messages are sent through the network from the source to the destination in order to discover and reserve paths which satisfy a given QoS requirement. Due to the dynamic nature of the network, reserved QoS paths must be reaffirmed periodically by sending special control packets, called *refreshers*, along the path. Another approach, called *soft state*, relies on periodic time out at each node for path maintenance. Algorithms that provide QoS support in MANETs should include the following features:

- Accurate measurement of bandwidth availability in the shared wireless channel and accurate measurement of effective end-to-end delay in an unsynchronized environment.
- Distributed routing algorithm that adapts with the dynamic environment.
- Resource reservation that guarantees the available resources
- Efficient resource release upon end of data transfer
- Authentication of the nodes during route discovery
- Security of the established route.

We used AODV routing protocol [3], to include all the features listed above. Extensions are added to the route discovery packets, specifying the service requirements that must be met by nodes re-broadcasting a Route Request (RREQ) or returning a Route Reply (RREP) for a destination. The algorithm proposed provides the option of performing QoS guided route discovery only when required and finding the shortest path otherwise.

2. QOS ROUTING PROTOCOL DESIGN CONSIDERATIONS

Due to the fact that network resources are very limited in MANETs, QoS routing is achieved with constraints on bandwidth, delay, jitter, packet loss rate and route stability. The characteristics of MANETs also determine the challenges in ad hoc QoS routing:

Volume: 03, Issue: 04, Pages:1253-1260 (2012)

- The link capacity is time-varying, which makes admission control difficult.
- Resource reservation is not stable, because the availability of the reserved bandwidth over shared medium is not guaranteed. As mentioned before, the communication capacity between nodes can dramatically change, which may result in QoS re-routing or routing recovery.
- Once a route fails, failure detection and recovery is required.
- End-to-end delay guarantee is not hard in an unsynchronized network.

T. Chen [4] proposed the Global State Routing (GSR) which maintains a global view of network topology and optimizes their routing decisions locally based on the link state vectors exchanged among the neighbor nodes during exchange of routing information. The exchange frequency of link state vectors depends on the node's distance to destination.

C. Lin *et al.* proposed a bandwidth routing protocol for QoS support in a multi-hop mobile network [5], contains end-to-end bandwidth calculation and allocation. The source is aware of the bandwidth and QoS available to all the destinations in the mobile network. This knowledge enables the establishment of QoS connections within the mobile network and the efficient support of real time applications.

A distributed QoS routing scheme is proposed in [6]. In the proposed algorithms, multiple paths are searched in parallel to find the best qualified, which is called "ticket based probing". The advantageous properties of the ticket-based probing include dynamic tradeoff between the overhead and the routing performance; working with imprecise state information; avoiding any centralized path computation that could be very expensive for QoS routing in large networks and the local and end-to-end states maintained at the intermediate nodes can be collectively used to direct the probes along the low-cost feasible paths toward the destination. Fault-tolerance techniques are employed in the scheme for the maintenance of the routing paths resulted from changes of network topology, which enable the proposed algorithms to tolerate high information imprecision. To improve the overall network utilization performance, a heuristic algorithm is proposed for the NP-complete delay-constrained and least-cost routing problem.

Ad hoc QoS On-demand routing (AQOR) [7] is a resource reservation-based routing and signaling algorithm that provides end-to-end QoS support. AQOR integrates on-demand route discovery between the source and destination; signaling functions for resource reservation and maintenance; and hop-by-hop routing. It introduces a detailed computation of available bandwidth and end-to-end delay. In traffic estimation and bandwidth availability, it considers both self traffic and neighbor traffic to reduce the hidden-node effect, which means that some bandwidth reserved at a certain node is for the traffic between neighboring nodes. AQOR estimates end-to-end downlink delay by measuring round trip delay. AQOR achieves *adaptive routing* by detecting QoS violations at the destination node or intermediate nodes.

CEDAR, a *Core-Extraction Distributed Ad hoc Routing* algorithm for QoS routing in a small to medium size ad hoc network is proposed in [8]. CEDAR dynamically establishes "a core of the network, and then incrementally propagates the link state of stable high bandwidth links to the nodes of the core. Route computation is on demand, and is performed by core nodes using only local state." The *advantages* of CEDAR include the facts that route discovery or maintenance duties are limited to a small number of core nodes, and link state propagation is a function of link stability or quality. The *disadvantages* of CEDAR are: core nodes have to handle additional traffic, which are associated with route discovery and maintenance; and it is hard to converge under high mobility.

QoS routing algorithms for mobile ad hoc networks proposed in the literature, sometimes directly use bandwidth as the metric to achieve QoS routing, and assume the link layer is capable of providing such bandwidth without considering the complexity of these assumptions. In addition, QoS support frameworks and differentiated services frameworks such as INSIGNIA also utilize hop-by-hop link layer bandwidth to check feasibility of routes and to reserve resources along the paths. Today MAC schemes for wireless ad hoc networks are not capable of providing QoS. Therefore, it is very important to design techniques and tools to study the effects of bandwidth sharing principles on the QoS.

3. QOS GUIDED ROUTE DISCOVERY

An important improvement over existing QoS algorithms is that the proposed algorithm provides the option for performing QoS guided route discovery only when required otherwise it finds the shortest path. An indication is sought from the input to the presence of QoS requiring applications. Conventionally, AODV uses hop-count as a parameter to choose between the routes available. We introduce the concept of QoS guided route discovery by making bandwidth, delay and jitter as the basis of the choice of route. This is implemented by appending the requested bandwidth, delay and jitter to the existing Route Request Header. As the request propagates through the nodes, they are checked for the availability of the required

resources. Only if the node can provide the minimum requirements specified in the request header, it forwards the request such as

- For bandwidth, the node's available bandwidth must be greater than or equal to the required bandwidth specified in the request header.
- For jitter and delay, two additional parameters are defined-accumulated delay and accumulated jitter. These are measures of the delay and jitter of the path. These are appended to the header and updated at every node.

The check is performed at the arrival of the request, after updating of the accumulated value. If the accumulated value exceeds the required delay and jitter values, the requests are discarded. Thus the request that reaches the destination first is the shortest route that satisfies the QoS requirements. The reply propagates through the reverse path as in normal AODV.

4. RESOURCE RESERVATION

The QoS guided route discovery is supplemented by resource reservation. Once the route is established, bandwidth is reserved for the particular service through the reply packet along the reverse route using a reserve flag. To guarantee the allocation of bandwidth, the available bandwidth at each node along the path is deducted by the requested bandwidth. If the route is selected by the source, data packets are transmitted and the bandwidth is efficiently released at the end of transmission through the de-reserve flag in the last data packet. Otherwise the reservation is automatically cancelled and the bandwidth released at each node upon the expiration of a timer set to $2T_{max}$ where T_{max} is the maximum accumulated delay in the path calculated during route discovery. The use of bandwidth reservation has greatly helped in reducing the packet end-to-end delay of data packets scoring highly over normal route discovery. The appropriate reduction in available bandwidth facilitates multiplexing service to more than one source helping in efficient use of resource.

5. QOS ROUTING METRICS

Let us assume that node m is one of node n's previous hop from the source S. Denote $T_n(m; j)$ as the trust on node m, assigned by node n, after the j-th topology updating cycle. Note that a simple way to measure $T_n(m; j)$is to compute the ratio of the number of messages correctly verified to the number of messages that have been attempted by using a statistics model as in [9]. Every time a new observation comes in, the node updates its repository and calculates a trust value by using a moving average model. After the $(j + 1)^{th}$ topology updating cycle, we can get

$$T_n(m; j) = \gamma \; T_n(m; j) + (1 - \gamma) \; T_n(m; j + 1) \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

where $T_n(m; j + 1)$ is node m's trust value measured by node n during the $(j + 1)^{th}$ topology updating cycle; $0 < \gamma < 1$ is a weighting factor used to trade off between current measurement and previous estimation.

Consider a path p that starts from a source node S to a destination node D. Let's denote $T_p(j)$ as the trust value of the path p. Since in path p, each node can choose one node from its routing table as its previous neighbor to forward route reply message (RREP). Then source S can use this path to send data packets. $T_p(j)$ can be expressed as

$$T_p(j) = \sum_{n,m \in p} \hat{T}_n(m; j) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

which serves as a security requirement on path p.
To consider link quality, we use the expected transmission count (ETX) proposed in [10] as a metric. Let's denote X the ETX, which can be expressed as

$$X = \frac{1}{d_f \times d_r} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

The forward delivery ratio, d_f, is the ratio of the number of packets received by a recipient to the total packets send out. The reverse delivery ratio, d_r, is the probability that an ACK packet is successfully received.

To consider QoS requirements, for example, packet delay for delay-sensitive traffic, we use d_n to represent the delay a packet experienced when being delivered to n by m. Thus, we can design a combined metric as follows:

$$\psi(p) = \sum_{n \in p} [\alpha X_n + (1 - \alpha) d_n] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

for p ∈ {all paths from S to D}, where $0 < \alpha < 1$ is a weighting factor used to trade off between link quality and packet delay requirements.

Considering both the security and performance requirements, a path that is less trusted and does not meet the desired performance must be penalized in our objective, thus a combined cost function can be designed as

$$D(p) = \beta \psi(p) + (1 - \beta)(1 - T_p(j)) \quad \ldots\ldots\ldots\ldots\ldots (5)$$

where $0 < \beta < 1$ is a coefficient used to weight among the performance and security requirements. Now the routing problem can be written as:

Min D(p), for p ∈ {all paths from s to x }……(6)

and subject to the constraints:

$X_n \geq 0$; $T_{min} \leq T_n(m; j)$; for n ∈ p……(7)

where T_{min} is the minimum trust required for a node to be allowed to join in a route. In equations (4) and (5), we explicitly integrate the security and QoS requirements. For a node n in path p, the values of X_n, d_n and $T_n(m; j)$ can be obtained. Therefore, node n can calculate the cost function $D(p)$ for its next hops and select a path that has the minimum $D(p)$.

6. ATTACKS ON QOS IN MANETS

We consider some of the attacks on QoS system.

***Attack model 1*:** Malicious alteration of non-mutable parameters in transmission. For example, an attacker can change the requested QoS in RREQ packets. It can also maliciously alter the QoS reservation parameters in RREP which will result in reservation of an incorrect amount of QoS resources.

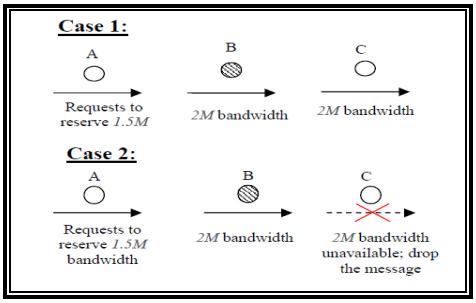

Fig. 1: An example of malicious alteration of non-mutable parameters

Figure 1 is an example of this attack: node A receives a signaling message from originator S to request a reservation of 1.5M bandwidth. Node B is an adversary residing adjacent to A on the route who maliciously alters the request for bandwidth to 2M, which is larger than the original request value. If the attack is successful, the downstream nodes would not be aware of the malicious alteration. Therefore they would reserve 2M bandwidth in case that there is 2M bandwidth available at each downstream node (case 1 in the figure 1); or some downstream node will drop the request message in case it cannot provide 2M bandwidth (case 2 in the figure 1), even if it is capable of providing 1.5M. If a malicious node decreases the value of the requested resources, it can result in a reservation of insufficient resources which can also disrupt the quality of the service provided to the flow from originator S.

***Attack model 2*:** Denial of QoS request. An adversary can potentially intercept or drop reservation messages so that the QoS reservation and the channel setup will be failed or tremendously delayed. This attack can prohibit the QoS resources from being available to the victim.

***Attack model 3*:** Intentional provision of fallacious QoS states information. Although QoS states information is subject to errors due to the rapid topology change and high node mobility, a deliberate distribution of false information will do more harm to QoS provisions.

Attack model 4: selfish nodes can severely degrade network performances and eventually partition the network by simply not participating to the network operation to save battery life for its own communication. This can endanger the correct network operation by simply not participating in the routing protocol or by not forwarding packets.

In this type of attacks, an adversary may tamper with the mutable QoS parameters in signaling messages in order to disrupt the measurement of QoS state and provide false information. The attacks may result in failure of resource reservation, insufficient or excess reservation. We have concentrated to eliminate the attack 1.

7. SECURITY MECHANISM FOR QOS IN MANETS

In QoS ad hoc networks, users need to assure the party who sent a signaling message is indeed the legitimate party and the malicious nodes should be eliminated. Otherwise, a malicious node can tamper QoS signaling messages with falsified data to steal or deplete resources used or reserved by other nodes. These attacks can result in degraded performance of networks, interference of resource reservation, unauthorized use of resources, or even failure of QoS provision.

7.1 Simple authentication to Secure QoS

To prevent the attacks on QoS parameters and to achieve secure QoS in MANETs, requires the network to provide authentication and digital signatures for the control packets; that is, any node that receives a request or reply packet must be able to ascertain that the claimed initiator sent it. An authentication protocol should be lightweight and impose as small computational and message overhead as possible due to the fact that resources in a mobile ad hoc network are very limited. In our scheme, we have used a RSA algorithm [11] for securing the QoS parameter – Bandwidth.

Before sending a RREQ message, the originator signs the QoS parameters with its private key. Each intermediate node on the path can *voluntarily* verify the digital signature to assure that the QoS parameters have not been maliciously altered during transmission. After the RREQ reaches the destination node, the destination checks the integrity of the non-mutable QoS objects via MAC verification. If the objects have been altered during transmission, the destination node will raise an alarm. Otherwise, it generates RREP packet, hashes the QoS parameters and sends it back to the originator of the request. The originator will verify the authentication and integrity of the QoS parameters upon receiving the RREQ packet from the destination. The End to End authentication is shown in the figure 2.
The end to end authentication algorithm is given as

A→B→C→D

- Let (BW XOR Dest.IP) = XYZ
- A sends RREQ by encrypting XYZ with public key, K_{public}
- (RREQ,Cipher) is transmitted to neighbouring nodes
- The node B can verify the RREQ, but fails to decrypt the cipher text, and sends to node C
- Similarly, node C can verify the RREQ, but fails to decrypt the cipher text
- Finally, the destination node receives the RREQ and decrypts the cipher text with its private key
- Plain text, $XYZ = C^e \pmod n$
- Performs XYZ XOR Dest.IP gives BW
- Verifies the BW mentioned in the RREQ
- If they match, the destination D encrypts the RREP and transmits to neighbouring nodes
- Otherwise D raise the alarm to neighbouring nodes

8. SIMULATION ENVIRONMENT AND RESULTS

The simulation for evaluating the performance of our proposal is implemented using the GloMoSim. Each simulation is executed for 600 seconds of simulation time. We have extended AODV codes to use QoS parameters to select a path based on MAC 802.11. In this work, we consider bandwidth, delay and jitter as the QoS metrics in our route discovery. In our simulation scenario, 50 mobile nodes move randomly in a 700 by 700 meter area at a speed of 5 metre/second. During 500 seconds of simulation, 3 source nodes send 4 constant bit rate traffic (varied between 100kbps and 1.8Mbps) to 4 destination nodes. We define a QoS evaluation metric, packet delay, which shows the average packet latency. We present the comparison of AODV and AODV with QoS protocols for different data traffic rates. The results shows that pausing the sessions in AODV with QoS does not add more latency on delivering the packets, but only prevents bandwidth congestions which results in a significantly shorter packet delay. Although the session will be delayed for the time the demanded QoS cannot be provided, the information carried will not be lost inefficiently. Also, we have varied the percentage of malicious nodes from 0% to 40%, and the density of networks is set to 16 (i.e. the

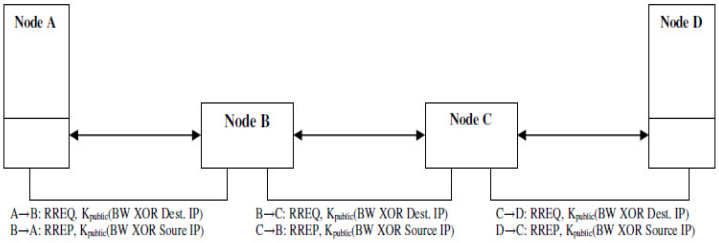

Fig.2: End to End authentication

nodes have an average of 15 neighbors), thus, network have a high probability to be connected to avoid side effects of isolated nodes and to sometimes provide alternate paths around malicious nodes. We evaluated the following performance metrics:

- **Average End-to-End Delay of Data Packets:** This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc.

- **Total overhead:** The ratio of the total packets transmitted (i.e., sum of control packets and data packets) to the data packets delivered.

- **Bandwidth cost for data:** The bandwidth cost for data is defined as the total number of data packets transmitted at all mobile hosts normalized by the total number of received data packets.

- **Mobility:** Mobility refers to the velocity with which a mobile node moves.

- **Routing Overhead:** Routing Overhead is the number of routing packets transmitted for every data packet sent. For the performance measurement, we have used the normalized routing load, which is the ratio of routing packets to the data packets transmitted.

- **Average route request hop-to-hop delay:** It is the average of the delays incurred by all the route request packets that are successfully transmitted hop-by-hop because our authentication algorithms impose delay penalty mainly on route requests.

As shown in Figure 3, the packet delay in AODV with QoS case stays below 40ms except after a rate of 1700 Kbps. Whereas, in the AODV case, the packet delay increases proportionally to the rate from 500Kbps to 1300 Kbps and then remains around 150 ms. The AODV with QoS packet delay is mostly lower than the AODV because the path selected to run the session with AODV with QoS has higher bandwidth efficiency due to reservation and therefore avoids congestion.

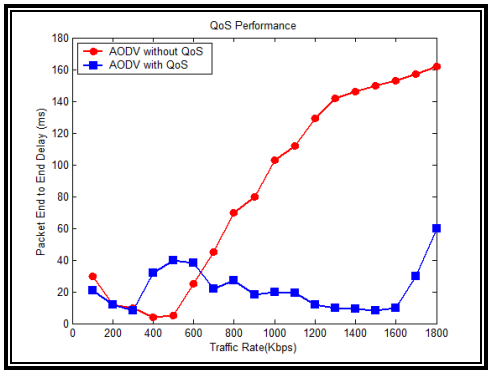

Fig. 3: Performance Evaluation for QoS Guided Route Discovery – Packet End-to-End Delay Vs Traffic Rate

The Figure 4 shows the comparison of average throughput of network under different speed with and without QoS. It has observed as the speed increases the throughput of the AODV with QoS is higher than the AODV without QoS. This is because in the case of AODV without QoS, as the speed increases the number of collisions and packet dropping are more which increase the route failures. Where as the AODV with QoS reserve the bandwidth, calculate the delay and jitter for the selected route before transferring the data into the networks. The number collisions and dropping of the data packets are also avoided, which in turn increases the throughput. Therefore the average throughput of AODV with QoS is higher than the AODV without QoS.

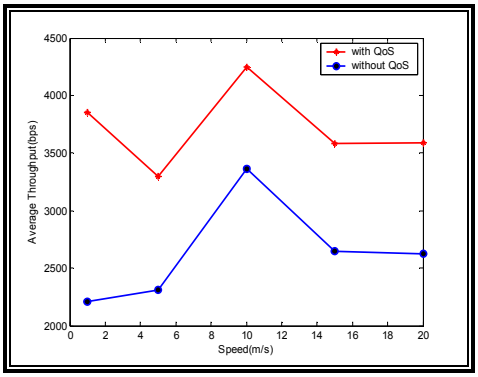

Fig. 4: Average Throughput Vs Speed

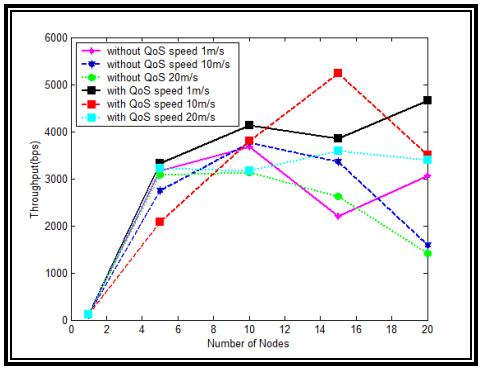

Fig. 5: Average Throughput Vs Number of Nodes

The Figure 5 presents the comparison of average throughput of network under different traffic with and without QoS. Without QoS, it was observed that when the mobility is less the increase in delay is not significant. Throughput is almost equal and the average throughput is increases to 90% as the traffic in the network increases for less speed and decreases to 70% as the speed increases from 1m/s to 20m/s. As the mobility increases, delay increases as a result the probability of all packets delivered in time at the receiver decreases. Hence the average throughput decreases as the speed of the mobile increases whereas in the case of AODV with QoS the throughput is high even though the speed increases form 1m/s to 20m/s. Hence, average throughput is higher for the AODV with QoS and routing efficiency of the protocol increases.

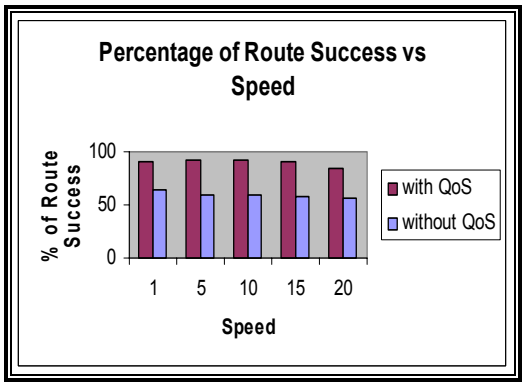

Fig. 6: Percentage of Route success Vs Speed

The Figure 6 shows the comparison of percentage of route success of network under different speed with and without QoS. The number of route failures is less in the case of AODV with QoS. The efficiency of AODV without QoS is less because as speed increases the number of collisions increases and results in a drop of data packets.

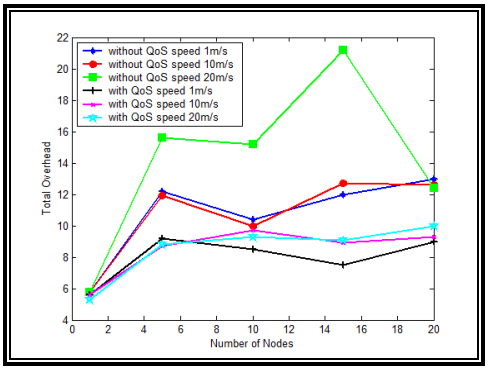

Fig. 7: Total Control Overhead Vs Number of Nodes

We can see from the Figure 7 the comparison of number of total control overhead with and without QoS. The figure shows that total control overhead for AODV with QoS is small for lower speed and slowly increases as the number of nodes and speed in the network increases from 1m/s to 20m/s.Whereas in the case of AODV without QoS the total control overhead is higher and increases, as speed and number of nodes increases. This is because in the AODV without QoS, the number of route failures increase as the speed of the mobile increases from 1m/s to 20m/s, which in turn increases the number of route discovery process.

Figure 8 shows the result of total bandwidth cost for data transmission. The bandwidth cost of data transmission for single source and destination is the smallest; while the bandwidth cost of data transmission for multiple traffic (randomly choosing a path) is the largest. This is because the unipath routing usually uses the optimal path from a source to a destination. The alternative paths in multiple traffic are usually suboptimal, which will cost more bandwidth. As the traffic increases, randomly choosing a path will cost more bandwidth than choosing a path based on its length.

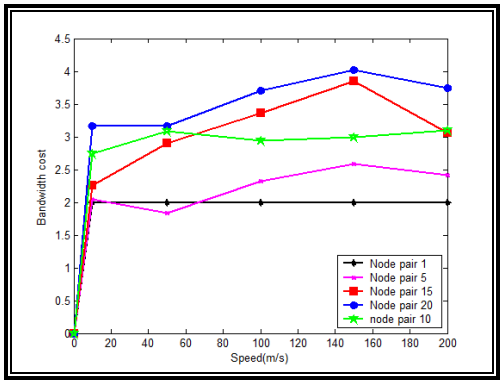

Fig. 8: Bandwidth Cost for data Vs Speed

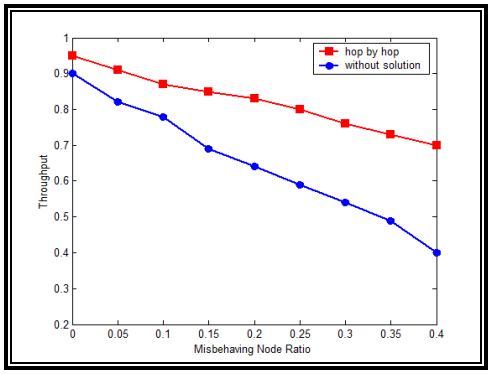

Fig.9: Misbehaving Node Ratio Vs Throughput

From the figure 9, the first thing that we can notice is that the throughput of the network degrades as the malicious nodes increases. Here we have varied malicious nodes upto 40%. With End to End authentication, the number of malicious nodes can be prevented and the throughput is increased.

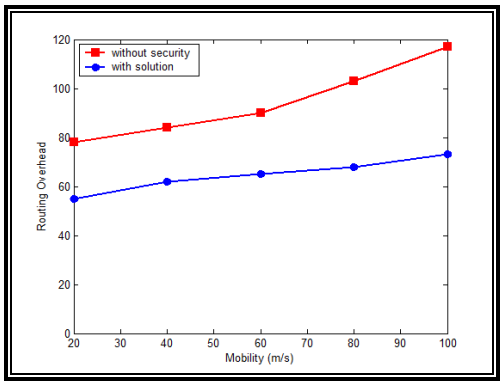

Fig. 10: Mobility Vs Routing Overhead

From figure 10, we have found that as mobility increases, the routing overhead increases due to malicious nodes and with the proposed solution, the routing overhead can be reduced.

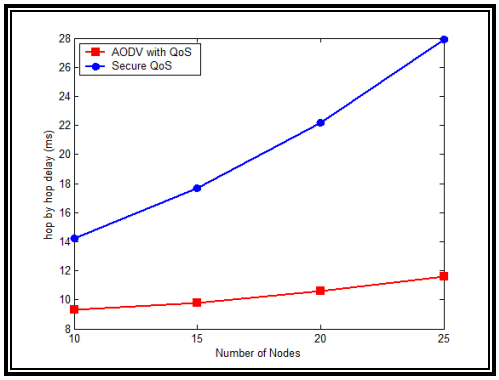

Fig. 11 : Average hop by hop delay of route request packets

We tested scenarios which include 10, 20 and 25 nodes respectively. The results of the QoS AODV and our security protocol are listed in Figure 11. From the figure we can see that the delay penalty imposed by our security mechanism is high compared with AODV QoS. This is due to that each node has to perform encryption and decryption of QoS parameters.

9. SUMMARY

In this work, we have introduced a routing protocol that provides per-flow end-to-end QoS support in MANETs in terms of bandwidth, end-to-end delay and jitter. It also facilitates the discovery of secure QoS parameter – bandwidth through authentication and by avoiding malicious nodes, thus protects against most of the security threats and attacks. Our simulation results show that we are able to secure the AODV protocol from End to end authentication and achieve increased Throughput, while keeping the Routing Overhead minimal. The results validate that our protocol can successfully provide sustainable and secure QoS support to multimedia applications with high reliability and low delay. As a future work, the work can be extended by eliminating selfish nodes by giving incentives.

REFERENCES

[1]. S. Chakrabarti., A. Mishra, “QoS issues in ad hoc wireless networks” IEEE Comm. Mag. 39, pages 142–148, 2001

[2]. S. Chen and K. Nahrstedt, “Distributed Quality-of-Service Routing in Ad Hoc Networks,” *IEEE JSAC*, vol. 17, pp. 1488–505, 1999

[3]. C. E. Perkins and Elizabeth M. Royer, "Ad hoc On-Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90-100, 1999

[4]. T. Chen, “Efficient Routing and Quality of Service Support for Ad Hoc Wireless Networks,” Ph.D. Dissertation, Computer Science Department, University of California at Los Angeles, Los Angeles, CA, 1998

[5]. C. Lin and J. Liu, "QoS Routing in Ad Hoc Wireless Networks," *IEEE on Selected Areas in Comm.* , vol. 17, no. 8, pp. 1426-1428, Aug 1999

[6]. S. Chen and K. Nahrstedt, “Distributed Quality-of-Service Routing in Ad Hoc Networks,” *IEEE JSAC*, vol. 17, pp. 1488–505, 1999

[7]. Q. Xue and A. Ganz, “Ad Hoc QoS On-demand Routing (AQOR) in Mobile Ad Hoc Networks,” *Journal of Parallel and Distributed Computing*, vol. 63, no. 2, pp. 154-165, February 2003

[8]. R. Sivakumar, P. Sinha and V. Bharghavan, “CEDAR: a Core-Extraction Distributed Ad Hoc Routing Algorithm,” *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1454-1465, August 1999

[9]. J. Dowling, E. Curran, R. Cunningham, and V. Cahil, ”Using Feedback in Collaborative Reinforcement Learning to Adaptively Optimize MANET Routing,” *IEEE Trans. on SMC, Part A: Systems and Humans*, pp. 360-372, vol. 35, no. 3, May 2005

[10]. D. De Couto, D. Aguayo, J. Bicket, and R. Morris, ”A High-Throughput Path Metric for Multi-Hop Wireless Routing”, *MOBICOM*, Sept. 2003

[11]. William Stallings, “Cryptography and Network Security – Principles and Practices”, 3rd edition, Person Education, 2004

Authors Biography

Dr.Ananda Krishna B graduated from Madras University in Electronics and Communication Engineering during the year 1999. He obtained his Master degree in Digital Electronics & Advanced Communication from Manipal Institute of Technology, Manipal and Ph.D in the area of Improving Quality of service through Secured Routing in Ad Hoc Networks at Jawaharlal Nehru Technological University, Hyderabad. Presently he is working as a Professor in the department of ECE at Gudlavalleru Engineering College, Krishna Dt. AP

Mr. R. Ramesh graduated from Bangalore University in Electronics and Communication Engineering during the year 1998. He obtained his Master degree in Digital Electronics & Advanced Communication from Manipal Institute of Technology, Manipal and his area of interest is Wireless Communication and Network Security. Presently he is working as an Assistant Professor Selection Grade in the department of ECE at SRM University, Chennai.