Volume 3, No. 4, April 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

PERFORMANCE BASED SECURE OPTIMIZED ROUTING PROTOCOL FOR MOBILE AD-HOC NETWORK

Anoop Kumar Jain[1], Sambhav Jain[2] and Anita Namdev[3]
[1]Dept. of Computer Application
Samrat Ashok Technological Institute, Vidisha (M.P.)
anoopjain0108@gmail.com
[2]Dept. of Information Technology
Shri Vaishnav Institute of Technology & Science, Indore (M.P.)
sambhav.jain43@gmail.com
[3]Dept. of Computer Science & Engineering
Laxmi Narayan College of Technology, Bhopal (M.P.)
namdevanita@gmail.com

Abstract- In mobile ad hoc networks (MANETs), accurate throughput-constrained Quality of Service (QoS) routing and admission control have proven difficult to achieve, mainly due to node mobility and contention for channel access. QoS related with band width utilization is very interesting because band width is the most critical resource in mobile ad hoc networks. The QoS issue must also be studied with a growing node density. This is because the beauty of attaining wider band width link is highly appreciated when the band width resource is scarce due to congestion and high traffic. In this paper, a comparative analysis of two proactive protocols: Destination Sequence Distance Vector (DSDV) and OLSR (Optimized Link State Routing) is conducted in their traditional best effort routing part. Evaluation of their performance is compared against with band width management metrics. Based on the result of the comparative analysis we develop secure QoS versions of the OLSR protocol. Algorithm is introduced that allow OLSR to find the maximum bandwidth path with optimal number of MPR (Multipoint Relay), show through simulation and proof that this algorithm does improve Secure Qos in the aspect of bandwidth. The simulation results show that our secure QoS versions of the OLSR routing protocol more efficient than existing works.

Keywords- MANET, Secure QoS, DSDV, OLSR.

INTRODUCTION

In ad-hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Therefore, routing protocols in ad-hoc networks must be adaptive to face frequent topology changes because of node mobility. Unlike conventional wireless networks, ad hoc networks have no fixed network infrastructure or administrative support. The topology of such networks changes dynamically as mobile nodes join or depart the network or radio links between nodes become unusable. Conventional wireless networks require as prerequisites a fixed network infrastructure with centralized administration for their operation.

Quality-of-service (QoS) routing in a MANET network is difficult because the network topology may change constantly and the available state information for routing is inherently indefinite. To support QoS, the link state information such as Bandwidth, Routing over head, Average End to end Delay (AED) and jitter in the network should be available and manageable. However, getting and managing the link state information in a MANET is by all means not simple because the quality of a wireless link changes with the surrounding circumstance. Furthermore, the resource limitations and the mobility of hosts add to the complexity [1] and [3].

However, the unpredictable nature of Ad-Hoc networks and the requirement of quick reaction to QoS routing demands make the idea of a proactive protocol more suitable. When a request arrives, the control layer can easily check if the pre-computed optimal route can satisfy such a request. Thus, waste of network resources when attempting to discover infeasible routes is avoided. Based on this consideration, in the thesis, we study the approach of pro-active QoS routing, and study two of the most common proactive protocols (DSDV) and OLSR Protocols. And modify a best-effort pro-active routing protocol OLSR for QoS purpose. The QoS requirement studied in the thesis is the bandwidth constraint [4].

Generally the Objective of this paper is to Study two common Proactive protocols (DSDV & OLSR) for secure QoS incorporation, selecting a protocol with promising performance for SECURE QOS, proposing and implementing BW aware route discovery for the selected protocol and study the performance achieved using simulation.

BACKGROUND SURVEY

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

© JGRCS 2010, All Rights Reserved

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. Each route update packet, in addition to the routing table information, also contains a unique sequence number assigned by the transmitter. The route labeled with the highest (i.e. most recent) sequence number is used. If two routes have the same sequence number then the route with the best metric (i.e. shortest route) is used. Based on the past history, the stations estimate the settling time of routes. The stations delay the transmission of a routing update by settling time so as to eliminate those updates that would occur if a better route were found very soon [1] and [2].

Optimized Link State Routing Protocol (OLSR):

Classic link-state algorithms declare all links with neighboring nodes and flood the entire network with routing messages. Optimized link-state routing compacts control packet size by declaring only *multipoint relay selectors*, a subset of neighboring links. To further reduce traffic, OLSR uses only the selected nodes, called *multipoint relays* (MPRs), to flood the network with routing messages. Each node selects a set of neighboring nodes as MPRs, and these nodes rebroadcast packets received from the originating node. Thus, unlike ordinary broadcast, not every node forwards routing messages. Each node maintains a table of MPR selectors and rebroadcasts every message coming from those selectors. In this way, the network distributes only partial link-state information, which OLSR can use to calculate an optimal route in terms of number of hops. Each node periodically broadcasts hello messages containing information about its neighbors and a link status. Nodes select the minimal subset of MPRs among one-hop neighbors to cover all nodes two hops away. Thus, every node in the two hop neighborhood must have a symmetric link to a given node's MPR set. Because OLSR significantly reduces the number of broadcast retransmissions, this algorithm is most effective in networks with dense node distribution and frequent communication [3] and [5].

QoS Routing:

"Quality of Service—the collective effect of service performance which determines the degree of satisfaction of a user of the service". The provisioning of QoS based network services is in general terms an extremely complex problem, and a significant part of this complexity lies in the routing layer [5]. The goals of QoS routing are twofold: selecting paths that can satisfy given QoS requirements of arriving communication requests, and achieving global efficiency in resource utilization. The following issues were addressed in QOS routing [5] and [6].

Dynamically Varying Network Topology: Since the nodes in an ad hoc wireless network do not have any restriction on mobility, the network topology changes dynamically. Hence the admitted QoS sessions may suffer due to frequent path breaks, thereby requiring such sessions to be re-established over new paths.

Imprecise State Information: The state information is inherently imprecise due to dynamic changes in network topology and channel characteristics. Hence routing decisions may not be accurate, resulting in some of the real-time packets missing their deadlines.

Lack of Central Coordination: Unlike wireless LANs and cellular networks, AWNs do not have central controllers to coordinate the activity of nodes. This further complicates QoS provisioning in AWNs.

Error Prone Shared Radio Channel: During propagation through the wireless medium the radio waves suffer from several impairments such as attenuation, multi-path propagation, and interference (from other wireless devices operating in the vicinity).

Hidden Terminal Problem: This problem occurs when packets originating from two or more sender nodes, which are not within the direct transmission range of each other, collide at a common receiver node.

Limited Resource Availability: Resources such as bandwidth, battery life, storage space, and processing capability are limited in AWNs. Insecure medium: Due to the broadcast nature of the wireless medium, communication through a wireless channel is highly insecure [4] and [7].

Need for Multipath Routing:

In case of the route failure, this single-path routing protocol initiates again another route discovery which put a massive load on the network. Single route to destination node increases the probability of a malicious node existence in discovered path. Single Path protocols learn routes and select a single best route to each destination. These protocols are incapable of load balancing traffic. Multi-path protocols learn routes and can select more than one path to a destination. These protocols are better for performing load balancing. Single-path inter-networks are not fault tolerant. Multipath internetworks are fault tolerant when dynamic routing is used. Also single path routing is less efficient in bandwidth aggregation and reduced delay when compared to mutipath routing.

Multipath routing allows the establishment of multiple paths between a pair of source and destination node. It is typically proposed in order to increase the reliability of data transmission or to provide load balancing and has received more and more attentions.

© JGRCS 2010, All Rights Reserved

In recent presented a new approach based on a mobile routing backbone for supporting Quality of Service (QoS) in MANETs. In real-life MANETs, nodes will possess different communication capabilities and processing characteristics. Hence, they aimed to identify those nodes whose capabilities and characteristics will enable them to take part in the mobile routing backbone and efficiently participate in the routing process. Moreover, the route discovery mechanism we developed for the mobile routing backbone dynamically distributes traffic within the network according to current network traffic levels and nodes' processing loads. Simulation results showed that their solution improved network throughput and packet delivery ratio by directing traffic through lowly congested regions of the network that are rich in resources. Moreover, their protocol incurs lower communication overheads than AODV (ad hoc on-demand distance vector routing protocol) when searching for routes in the network [6]. But this scheme is operated on single path. If the multipath routing is used, it will improve the reliability and throughput and favors load balancing. So, in this paper, we tend to extend this scheme over multipath routing protocol [1] and [8].

RELATED WORKS

OLSR-based QoS Routing:

In previous method integrated QoS features into the Optimized Link State Routing (OLSR) protocol to find a path with larger bandwidth. This approach does not modify the routing scheme of OLSR, but it chooses the different criteria to set the multipoint relays (MPR) set so as to find a larger bandwidth path.

OLSR is an optimization of the classical link state flooding algorithm. In OLSR, a set of nodes is chosen to form an MPR set such that broadcast packets are forwarded only among the MPR set. In this way, overhead is reduced significantly compared with classical flooding where every node needs to forward broadcast packets. Therefore, how to choose the MPR set is the key point of the OLSR algorithm. In the OLSR IETF draft, the one-hop neighbors that cover more two-hop neighbors are elected to the MPR set, in order to minimize the number of MPRs. Using this scheme for MPR election, it is quite possible that the low available bandwidth nodes will be chosen for the MPR set, which causes the routes to go through nodes with low available bandwidth.

Recently, presented quality of service (QoS) metrics for various network applications based on human factors and technology attributes. The first term, human factors, addresses human perception of different kinds of media, such as conventional text, audio and video. The second term, technology attributes, represented the different technological aspects of these network applications, such as time dependence and symmetry. Both of these terms were the key factors that lead to variations of requirements for QoS. Establishing these requirements is paramount to providing QoS on computer networks and the Internet. With the metrics presented in the proposed paper they provided the criteria necessary for such QoS assurance [2] and [7] and [9].

Ad Hoc QoS On-demand routing

It is a QoS-aware routing protocol with the following features: (1) available bandwidth estimation and end-to-end delay measurement, (2) bandwidth reservation, and (3) adaptive route recovery.

This routing is an on-demand QoS-aware routing protocol. When a route is needed, the source host initiates a route request, in which the bandwidth and delay requirements are specified. The intermediate hosts check their available bandwidth and perform bandwidth admission hop-by-hop. If the bandwidth at the intermediate host is sufficient to support the request, an entry will be created in the routing table with an expiration time. If the reply packet does not arrive in the allotted time, the entry will be deleted. Using this approach, a reply packet whose delay exceeds the requirement will be deleted immediately in order to reduce overhead.

To estimate available bandwidth for assisting in call admission, each node puts its reserved bandwidth in periodic Hello messages that are sent to their neighbors. It uses the sum of a node's neighbors' traffic as the estimated total traffic affecting the node. Note that this estimated traffic can be larger than the real overall traffic. This overestimation imposes a stringent bandwidth admission control threshold. The available bandwidth is thus a lower bound on the real available bandwidth. End-to-end one way downstream delay is approximated by using half the round trip delay. With the knowledge of available bandwidth and end-to-end delay, the smallest delay path with sufficient bandwidth is chosen as the QoS route.

Temporary reservation is used to free the reserved resources efficiently at each node when the existing routes are broken. If a node does not receive data packets in a certain interval, the node immediately invalidates the reservation. This avoids using explicit resource release control packets upon route changes. The adaptive route recovery procedure includes detection of broken links and triggered route recovery at the destination, which occurs when the destination node detects a QoS violation or a time-out of the destination's resource reservation. In this paper is to Study two common Proactive protocols (DSDV & OLSR) for secure QoS incorporation, selecting a protocol with promising performance for SECURE QOS, proposing and implementing BW aware route discovery for the selected protocol and study the performance achieved using simulation [8] and [10].

PROPOSED TECHNIQUES

A DSDV protocol is viewed to associate with so many problems as mentioned above and is seen to perform low especially with high node density and mobility. Therefore it is not reliable to incorporate QoS for DSDV. This is because DSDV does not guarantee assurance of enhancing the band width management metrics, packet delivery fraction and Goodput. Moreover the unpredictable nature of Ad-Hoc networks and the requirement of quick reaction to QoS routing demands make the idea of a "link-optimization routing" protocol more suitable. When a request arrives, the control layer can easily check if the pre-computed optimal

© JGRCS 2010, All Rights Reserved

route can satisfy such a request. Thus, wasting network resources when attempting to discover feasible routes can be avoided. Based on this consideration, unlike DSDV QoS routing protocols, we are studying "link-optimization routing". The task is to re-compute a route, which is the best route, based on the Secure Qos constraint among all the possible routes. The approach followed in this thesis work is to integrate the Secure Qos feature into OLSR, which is a pro-active routing protocol in a way optimal and more effective than other approaches. In simulations, we will first show that the traditional best effort OLSR outsmart the DSDV in band width management metrics, packet delivery fraction and goodput. We then incorporate Secure Qos into the promising OLSR, see the simulation and justify the results.

The main objective of this thesis is to incorporate Secure Qos into traditional best effort OLSR so as to obtain enhanced performance. A different approach is followed in both the MPR selection and route table computations from the OLSR. The new Secure Qos OLSR proposed here computes the optimal number of MPR based on its own new way of computing MPR and employs a route table computation that best suits the MPR (Multipoint Relay) selection.

Design of Proposed Algorithm:

The idea behind this algorithm for New Secure Qos OLSR is to select the highest bandwidth neighbors with optimal number of MPR: (N and N2 denotes all the 1 hop and 2 hop neighbor of the source node respectively)

a. Start with an empty MPR set
b. Select as MPRs nodes in neighbors N which provide the only path to some nodes in 2-hop neighbors N2
c. While there exist nodes in N2 which are not covered

{

a) 3.1. Select as MPR a node that has the highest bandwidth link connected with the current node and minimum possible set of MPR.
b) 3.2. Mark the neighbors of the newly selected MPR as covered in the 2-hop neighbor set of the current node

}

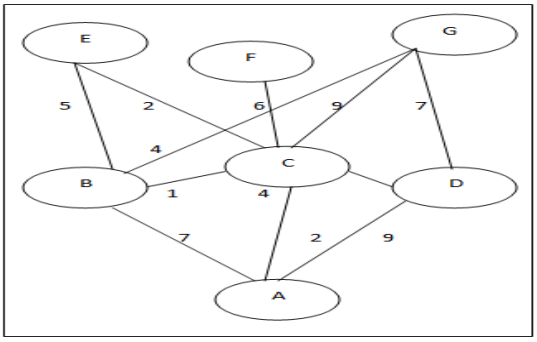

Figure 1: New MPR Selection

Among node A's neighbors, B, C, and D have a connection to its 2-hop neighbors. Among them, even if link AD has the largest bandwidth we choose node B. This will reduce the number of MPR and maintain selection of optimal wider link band width. So B is first selected as A.s MPR, and the 2-hop Neighbor E & G are covered. Similarly, C is selected as MPR and F is covered, so all 2-hop neighbors are covered and the algorithm terminates.

Available link band width calculation:

Secure Qos OLSR uses the media idle time to reflect the available bandwidth over a link. If the node is sending packets, its transmitter becomes busy. If there are other nodes beginning transmission within the interference range of the current node, its receiver senses the busy media and sends a media busy signal. As the MAC Layer already defines functionalities to capture changes of the media, the available link bandwidth is computed: Each node is randomly assigned an idle time ranging from 0 to 1. The available link bandwidth between two nodes is equal to the minimum of their idle time multiplied by the maximum bandwidth. Here, we consider that in the Ad-Hoc network, each link has the same maximum bandwidth, 2 Mbps. For example, if node A's idle time is 0.5 and node B's idle time is 0.3, then the available bandwidth over link AB is: 0.3 *2Mbps = 600 kbps. These randomly generated idle times reflect the traffic condition in the network snapshot because the consumed bandwidth over each link reflects the traffic flows over that link.

Performance Evaluation Metrics:

The metrics have been chosen in order to evaluate the routing protocols for Secure Qos in terms of wider link band width measured as Goodput, low percentage of packet loss and low routing load. The main attention was given to evaluate the routing layer performances. This is because Goodput alone does not indicate whether a protocol A is better than a protocol B. How it achieves higher Goodput when combined with scalability is a good measure of a better performance. [29] The following three metrics capture the most basic overall performance of Routing protocols studied in this thesis work: -

Good put:

Good put is defined as the amount of useful data, or payload that can be processed by, passed through, or otherwise put through a system when operating at maximum capacity and received at the correct destination address. Goodput can be thought of as throughput seen by the receiver.

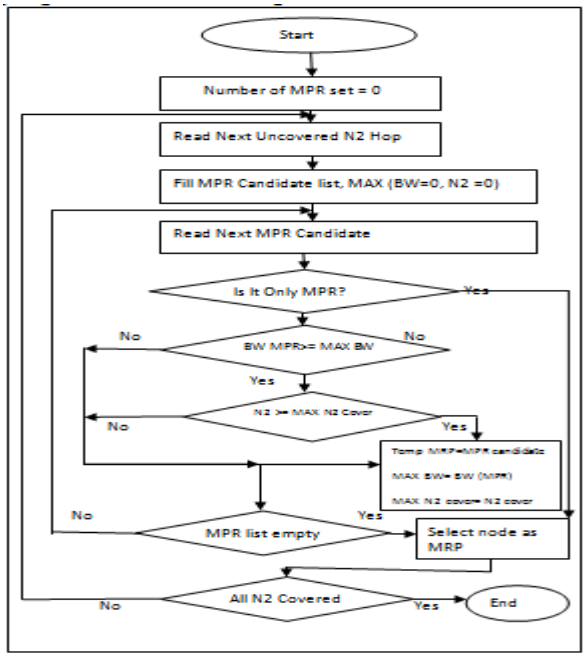

Figure 2: Flow Chart Secure Qos OLSR

© JGRCS 2010, All Rights Reserved

$$\text{Goodput} = \frac{(\text{max no of pkts recvd by the Rx in sequence}) * \text{packet size}}{\text{Measurement interval}}$$

Packet Delivery Fraction:

The packet delivery ratio in this simulation is defined as the ratio between the number of packets sent by constant bit rate sources and the number of packets received by the CBR sink at destination.

$$\text{Packet Delivery Fraction (PDF)} = \frac{\text{CBR packets received by CBR sinks}}{\text{CBR packets sent by CBR sources}}$$

Normalized Routing Load (NRL):

Routing overhead is the number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

$$\text{Normalized Routing load} = \frac{\text{Number of Routing Packets sent}}{\text{Number of Data Packets Received}}$$

Average End-to-End Delay of data packets (AED):

The end-to-end delay is defined as time between the point in time the source want to send a packet and the moment the packet reaches it destination. It includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

Average end to end Delay

$$= \sum \frac{T(\text{destination receives packet}) - T(\text{source wants to sent packet})}{\text{Number of Packets}}$$

SIMULATION ENVIRONMENT & RESULTS ANALYSIS

In this paper we implement secure QoS OLSR and secure OLSR all are executed in the same environment for comparison purposes in NS-2. The following choices are made for simulation considering accuracy of result and available resources. Then, we carry out quantitative and comprehensive evaluation of performance. The simulation parameters of our thesis work as follows:

Table 1 Simulation parameters

Length of MANET	300 (M)
No. of mobile nodes	60
Packet rate of normal connection	1
Movement Model	Random Waypoint
Traffic type	CBR, HTTP, FTP
Max. mode speed	5 m/s – 30 m/s
No. of connections between nodes	5 – 30
Pause time	10 s
Rate (packet per sec)	2 packets/s
Data payload (packet size)	64 – 512 bytes

In this Scenario the behavior of both algorithms secure OLSR and secure QoS OLSR is compared and contrasted by varying node density under different speed scenarios. The metrics to be analyzed are Goodput, Packet Delivery Fraction, and Average End to End Delay (AED). The size of nodes to be taken is 30, 40, 50 and 60.

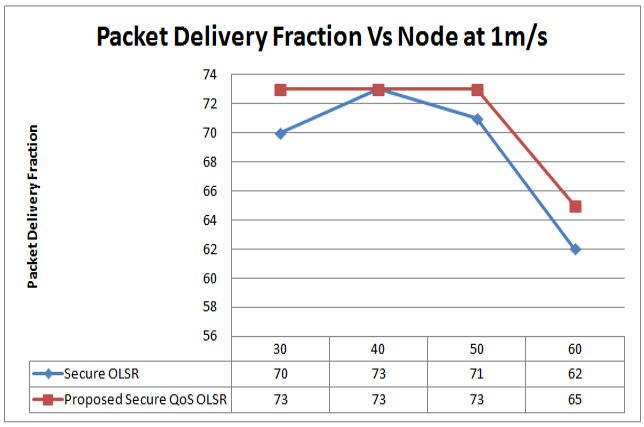

Figure 3 Packet Delivery Fraction Vs Node at 1m/s

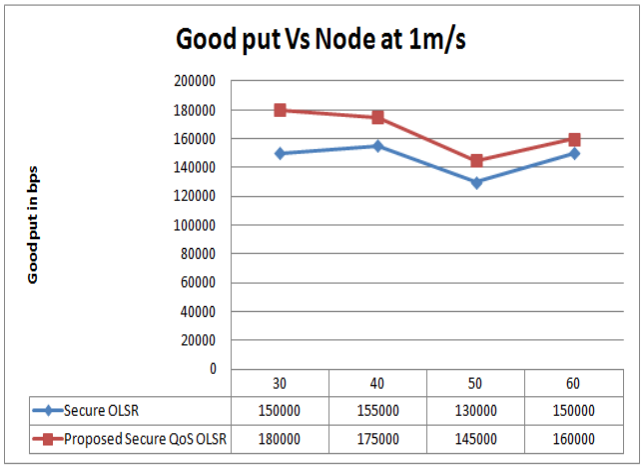

Figure 4 Good put Vs Node at 1m/s

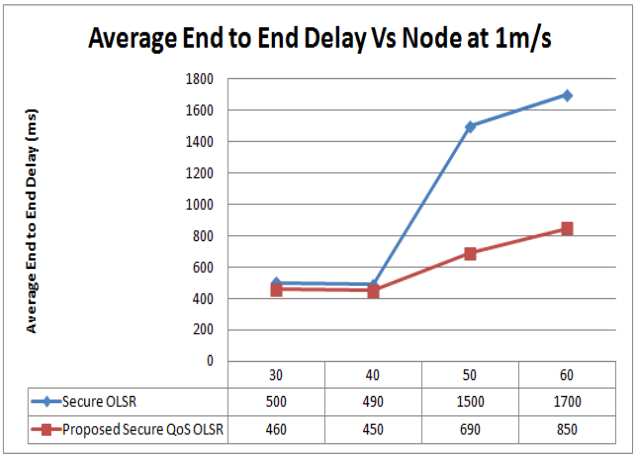

Figure 5 Average End to End Delay Vs Node at 1m/s

The Packet Delivery Fraction (figure 3) and Good-put (Figure 4) are both showing improvement with the secure QOLSR at this speed scenario because the secure QOLSR searches for a wider band width link and hence can transfer more packets to the destination and similarly can transfer data bits better than the OLSR. A maximum of 3.52 % and 16.75 % improvements are seen (at node 30) in Packet Delivery Fraction and Good-put respectively. Since secure QOLSR performs better in delivering packets and data bits than OLSR by selecting better link which is comparatively less congested.

In some cases the secure QOLSR shows better figure in Average End to End Delay (figure 5) metrics this can be

© JGRCS 2010, All Rights Reserved

explained by the fact that the algorithms in search of better link band width will transfer its packets in reduced end to end average Delay.

CONCLUSION

In this paper work, the principles of mobile ad hoc networks focusing on how to incorporate secure Qos will discussed. The importance of band width management Secure Qos metrics in growing node density and mobility is significant in mobile Ad-Hoc network. Two of the most commonly use Proactive routing protocols DSDV and OLSR protocols are studied. In order to decide which of the two proactive protocols Secure Qos will suit more, several literature reviews have been reviewed and comparative analysis. Both the reviewed literature and the results of the comparative analysis have proved OLSR to be a promising candidate to best perform in Secure Qos incorporation. This is because the band width management metrics have shown promising figures in OLSR than in DSDV and it is this set of Metrics that the thesis work is working up on. We will discuss in detail our idea of adding Secure Qos into the OLSR protocol. Our algorithm allows OLSR to find the maximum bandwidth path with optimal number of MPR.

REFERENCES

[1]. J.Premalatha and P.Balasubramanie, "Enhancing Quality of Service in MANETS by Effective Routing", 2010 IEEE ICWCSC.

[2]. Dr Chandra Shekar Reddy Putta,Dr K.Bhanu Prasad ,Dilli Ravilla, "Performance of Ad hoc Network Routing Protocols in IEEE 802.11", IEEE 2010 International Conf. on Computer & Communication Technology, pp 371-376.

[3]. Ze Li and Haiying Shen, "A QoS-oriented Distributed Routing Protocol for Hybrid Networks", IEEE 2010, pp 281-291.

[4]. Soumya Maity, P. Bera , and S. K. Ghosh, "An Access Control Framework for Semi-infrastructured Ad Hoc Networks", IEEE 2010 2nd International Conference on Computer Technology and Development (ICCTD 2010), pp. 708-712.

[5]. H. Wen, P.-H. Ho, C. Qi, and G. Gong, "Physical layer assisted authentication for distributed ad hoc wireless sensor networks", IEEE 2010, Special Issue on Multi-Agent & Distributed Information Security, pp. 390-396.

[6]. N H Ayachit, Santosh L Deshpande, and Kamakshi Prasad V, "Evolutionary Computing based secure key management Protocol", IEEE 2010.

[7]. Jinxia Yu, Yongli Tang, Xiancha Chen and Wenjing Liu, "Choice Mechanism of Proposal Distribution in Particle Filter", IEEE 2010, Proceedings of the 8th World Congress on Intelligent Control and Automation, pp. 1051-1056.

[8]. Amanda Peart, Mo Adda, "Quality of Service: Dynamic Authentication Bandwidth Management for the Wireless Environment", IEEE International Conference on Information Science and Engineering (ICISE2009), pp 5366-5369.

[9]. Bing He and Dharma P. Agrawal, "An Identity-based Authentication and Key Establishment Scheme for Multi-operator Maintained Wireless Mesh Networks", IEEE 2010, pp 71-78.

[10]. Hanal ABUZANAT, Benoit TROUILLET and Armand TOGUYENI, "Fair Queuing Model for EDCA to optimize QoS in Ad-hoc Wireless Network" , IEEE 2009 Eighth International Conference on Networks, pp 306-311.

© JGRCS 2010, All Rights Reserved