SECURE AND QUALITY OF SERVICE ORIENTED ROUTING PROTOCOL FOR MOBILE ADHOC NETWORKS

A
Report
on the
Major Research Project

Submitted to

UNIVERSITY GRANTS COMMISION

NEW DELHI

By

Dr. AJAY KOUL

Principal Investigator & Assistant Professor

School of Computer Science and Engineering

Shri Mata Vaishno Devi University

Katra (J&K), India-182320
2012-2015

Acknowledgement

I would like to express my deep sense of gratitude to University Grants Commission, New Delhi, for sanctioning this Major Research project "Secure and QoS oriented Routing protocol for MANETs" and for the financial support extended for completing this work.

I am highly thankful to **Prof. Sudhir K. Jain, Vice-Chancellor,** Shri Mata Vaishno Devi University, for providing the infrastructural facilities and all the amenities for the conduct of the study.

I am also thankful to my project fellows, colleagues, and office staffs of my department for their valuable suggestions and help to finish this report.

Dr. Ajay Kaul

Abstract

Mobile Adhoc network (MANET) is a highly dynamic, self configuring and decentralized network, which needs pragmatic and flexible approach to become operative in the severest kind of environment. Data transfer through this Ad hoc wireless network is required when it is hard to establish the large infrastructure. In MANETs there are many challenges in terms of deploying security especially when the confidentiality of the data is compromised. If the data is highly confidential, then providing security especially in the malicious environment is really a challenging task. Many researchers have however proposed solutions for internal as well as external attacks. But unfortunately everyone has some tradeoffs. Some methods are designed only for specific attacks. Some provide solutions for many attacks but depend on the factors like delay, high resource utilization etc. Researchers are working on securing MANETs by implementing more and more complex techniques like cryptography, digital signatures, hashing etc. These empirical techniques are highly effective in providing security but also have major influences over throughput, excellences of the system, sustain high cost and thereby degrade the Quality of Service (QoS). To improve the performance of MANETs in terms of end-to-end delay, throughput, least resource exploitation, least information loss etc. a different approach of deploying security in MANETs is required without sacrificing the QoS parameters.

List of Tables

List of Figures

List of Abbreviations

MANETs	Mobile Ad hoc Networks
QoS	Quality of Service
AODV	Ad hoc On Demand Distance Vector
DSR	Destination source routing
ZRP	Zone Routing Protocol
IntServ	Integrated Service
DiffServ	Differentiated Service
RSVP	Resource Reservation Protocol
SLA	Service Level Agreement
FQMM	Flexible QoS Model for MANETs
INSIGNIA	Signalling Protocol
SWAN	Service Differentiation in Wireless Networks
LWQ	Light weight QoS
HQMM	Hybrid QoS Model for MANET
AQOS	Adhoc Quality of Service
CEDAR	Core Extraction Distributed Ad hoc Routing
QoLSR	Quality of Service oriented Link State Routing
QoS-AODV	Quality of Service Adhoc on Demand Distance Vector
ARAN	Authenticated Routing for Ad hoc Network
SRP	Secure Routing Protocol
SAR	Security Aware Ad hoc Routing
SEAD	Secure Efficient Ad hoc Distance Vector

CONFIDENT	Cooperation of Nodes in Dynamic Ad hoc Networks
2ACK	2 Acknowledgement
SAODV	Secure Adhoc on Demand Distance Vector
SLSP	Secure Link State Protocol
SEDYMO	Secure Dynamic Mobile Environment
SEEEP	Simple and Efficient End to End protocol
S-DSDV	Secure Dynamic Source Distance Vector
SSM	System Security Module
DSM	Data Security Module
RM	QoS Routing Module
SNR	Signal to Noise Ratio
RSSI	Received Signal Strength Indicator
RREQ	Route Request
RREP	Route Reply
RTS	Reply to send
CTS	Clear to send
AOMDV	Adhoc on Demand Multipath Distance Vector
DSPLIT	Double Split
TORA	Temporary Ordered Routing Algorithm
SQRP	Secure QoS Routing Protocol

Standard Notations

$\subset$	Proper subset.
$\leq$	Less than or equal to.
$\geq$	Greater than or equal to
$\|xy\|$	Distance between points x and y
ϵ	Belongs to
$[x]_A$	Equivalence class of x in A
$f(x)$	A polynomial function
f_i	Function to work for data path for index i
$\bar{f}_i$	Function to work for monitoring reverse path for index i
$\tilde{A}$	Function to work for monitoring reverse path for index i

Table of Contents

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Mobile Ad hoc Networks (MANETs) are recognized for setting up inexpensive and temporary wireless communication systems without any premeditation. It is all because of its dynamic, self-configuring and decentralized nature. It is needed when we required setting up an Ad hoc network (without any preexisting infrastructure) immediately for performing communications and sharing important information over remote areas. Like in critical situations an application is needed to perform search and rescue operations (e.g. in a far flung region, it lacks the required infrastructure for effective communication or already deployed infrastructure is destroyed). There are other so many applications including disaster management, in wars, in medical field, in space programs like robots working on mars and sending information to the space centers on earth, in Health monitoring systems, in conferences, meeting rooms, virtual classrooms, in vehicular applications, traffic signaling etc. MANETs can be operating with heterogeneous devices. The unpredictable topologies in MANETs and its assorted nature are very challenging because it requires more responsiveness and maintenance time to time.

To make it work in well-organized way, the discovery of shortest and least congested routes in the varying topologies need to figure out first. But here lies another problem that MANET uses the wireless shared medium and where there is a shared medium there are chances of interference, snooping and annihilation of information as well as the network's physical entities. So it raised the need for data's confidentiality and integrity before exchanging it in the network and also the system's physical security. There are many other immense challenges and security requirements which we need to contemplate before deploying MANETs. Many researchers proposed their solutions [1], [2] which provide excellent security but they require very complex computations and consume a lot of resources like memory, bandwidth etc.

They have reduced the effect of various attacks but still they are insufficient and become compromised in some attacks [3], [4]. Other solutions [5], [6], [7], [8] are better in terms of providing some extent of quality of services (low memory utilization, low bandwidth, low power etc.) but they are also promising with certain type of attacks [6], [7]. This has become a big tradeoff between choosing those secured methods that consume a huge amount of resources (large memory, high bandwidth utilization and heavy processors for high computations), and those methods that consume fewer resources but are susceptible to various attacks.

In MANET, Quality of service (QoS) is the check maintained by the established network to assure best quality producing results to its users as per their requirements. This check is satisfied by setting some quality parameters (minimum throughput, minimum/maximum packet delay, minimum/maximum packet loss, minimum/maximum hop counts etc. according to the application's requirements). E.g. for multimedia delay sensitive applications, network must satisfy the minimum delay and minimum bandwidth requirements. But due to shared wireless medium and dynamic network topology of MANETs, it is very problematic to satisfy all quality bounds at one time. Though there are many ways of attaining QoS in MANETs by implementing it on all layers of OSI. Like in medium access control (MAC) layer, it is determined that which next node among the competing nodes should broadcast its packets on the shared wireless channel. Lately, much effort has also been focused on designing MAC protocols for the efficient utilization and allocation of resources on MAC layer.

After getting through many research papers which have discussed about MANET's deployment, routing, security, QoS features and issues etc. It is clear that infrastructure-less networks, MANETs are only established when some specific application needs to perform for solving some kind of problem. So, before raising an infrastructure-less network, we need to confine and find out what are our needs and what do we actually want from the network. For example, if an application needs certain bandwidth over some specific time schedule and cannot share it with anyone then it can be at least realized that the application needs a hard QoS approach. Likewise applications that have more concern over security of its data with delay constraints need to work on MAC layer and network layer. It requires following coupled and dependent QoS approaches.

This distinct approach can minimize the overhead of optimizing all layers of OSI and the consequent costs too. Therefore, a QoS model for a specific application can be proposed with or without being transparent to underlying protocols. One can work on managing the intake of flow of admissions in application and session layers which can positively reduce the overload on other layers. Priorities can also be set for admissions of flows. An existing routing protocol can be modified or extended while preserving its basic features.

Like flooding protocol is best known for its assured end-to-end packet delivery but its main issue is redundancy of packets in the network which can cause congestion. The basic feature of this protocol can be implemented into the QoS scheme with some modifications in its routing procedure so that least resources get consumed for end-to-end packet delivery. Choosing an appropriate routing protocol is another task for fulfilling the application's needs and QoS constraints in network. Remember that there is a big difference between choosing shortest path and QoS path. It is because shortest path may lead to the destination earlier but might be it is using the scarce resources in higher rate. Whereas QoS path may not be the shortest path but it can be the most feasible path in terms of bandwidth, power and other limited resources usage.

Several routing protocols are available which can provide the shortest routes but this does not mean that they also provide QoS. On choosing the right routing protocol we can estimate about which QoS constraints it can satisfy, what new metrics need to add and what other methods need to implement or what existed features need to modify. Transport layer protocols can also be considered because on that layer it is important to know if there is any packet loss and if yes, then is there any errors or packets are dropping due to congestion. Similarly, MAC protocols should also be carefully chosen so that hidden and exposed nodes problem can be avoided.

On physical layer, the most considerable part is to reduce the effects of fading, shadowing, noise and other distortions; minimizing and maximizing the use of power resource etc. After development of whole view of the QoS scheme, more improvements can be done by executing it in the worst environment and making it vulnerable to scarcity of resources, power etc. because it may help in finding out the pros and cons of our scheme before anyone criticized it. So on further steps can be taken accordingly. One more thing is assumptions should be made as less as possible because it generates the doubtful possibilities.

CHAPTER 2

MOTIVATION

Mobile Adhoc networks are recognized as self configuring and self-organizing network that is inexpensive and temporary wireless communication system without any predefined infrastructure. So it is needed to build a network that is secured as well as provide high quality of service for communication in critical situations. Quality of Service for a network is a guaranteed delivery of data which a network transfers from one region to another during a certain time. The QOS is a set of measurable service requirements of network such as delay, bandwidth of link, probability of packet loss, and jitter etc. Thus, a network needs to meet these requirements while transporting fragments from source to destination as well as Focusing upon maximum route availabilities and finding shortest route among them.

Routing protocol defines a mechanism to establish an optimal and efficient route for packets from source to destination in a network. As compare to single path from source to destination multipathing mechanism achieves higher degree of fault tolerance, load balancing due to multiple paths as if routing load is higher and there are frequently high rate of link failures, then performance of network goes slightly down as well as aggregation of bandwidth which increases the throughput as well as lifetime of network. Various variables such as environment, area, range, quality of service and security are critical in nature that affects the security in the network. To eliminate the redundancy or duplicity of data and to provide data level security and integrity, also a security approach is adopted.

The main aim is to develop both features i.e. security as well as good Quality of Services so that the protocol can combat maximum of threats on security of MANETs without deteriorating its proficiency of providing maximum throughput, minimum overall delay, lower bandwidth, power and memory consumption etc.

CHAPTER 3

LITERATURE REVIEW

The use of frequently changing wireless links in MANETs makes it susceptible to attack. So, the first step before sharing information is to discover the most secured routes which can be only accessed by the authorized users. Many protocols proposed claim their approaches to be most secured. Security routing protocols can be cryptographic based, trust based, observation based, reputation based and others. In cryptographic based techniques asymmetric and symmetric keys are distributed among nodes to protect the messages from being tampering and losing their integrity. But encryption/decryption schemes are not suitable for resource-constrained devices.

The key distribution schemes reduce overall efficiency in terms of memory, processing computations, power etc. Protocols using only cryptographic mechanisms may run out of resources and fall under the resource consumption attack. In trust and observation based schemes nodes and their neighbors are observed. The information to and from the observed nodes are stored in tables for further observations. These tables are periodically updated to avoid the stale information. In reputation based schemes ranks or reputation values to each node are already given. There is a predefined threshold value according to which reputation of each node is increased or decreased. There are certain hybrid approaches in which combination of the above schemes can be used.

3.1 WATCHDOG & PATHRATER

The positive aspects of watchdog and Pathrater [9] are that it can identify misbehavior at the forwarding level and not just the link level. This method works best when both watchdog and Pathrater are coordinating and watchdog performs best on top of a source routing protocol because the packet in transit knows it's previous and next hop address. There are also some negative sides of this method. Misbehaving node can confines its transmission power such that the true recipient gets too weak signal. This hints the misbehaving node identify the transmission power required to reach each of its neighboring nodes. Watchdog cannot notice multiple colluding nodes if they are dropping packets at a rate lesser than the preconfigured minimum misbehavior threshold. It requires

maintaining a lot of state info at each node as it observes its neighbors to confirm that they do not retransmit a packet that they have previously forwarded. When collision occurs at receiver end, retransmission of packet occurs, which may appear as a replay attack to node performing as watchdog. But the question arises here is that how to know nodes are misbehaving due to their own fault or they have been attacked? Because if we increase the negative values of malfunctioning nodes (trusted nodes) then the chances of the attacks by malfunctioning attacker nodes (working with the trusted ones) would also increase. Watchdog on its own does not affect routing judgments, but it deliveries Pathrater with additional information to fight misbehaving nodes more effectively and Pathrater alone cannot identify a path with misbehaving nodes to decrement its rate. Any route requests triggered by SRR can overflow the network with Route Request and Route Reply packets, which really increase the overhead. False positives occur when the watchdog mechanism reports that a node is misbehaving when actually it is not. If there are multiple paths then the path with high metric is selected whereas former picks whatever the shortest path available in the route cache.

3.2 SECURITY AWARE ROUTING PROTOCOL (SAR)

SAR [10] permits the use of security as a negotiable metric to improve the importance of the routes. As compared to AODV, this protocol sends less routing control messages. Fewer routes discover but these routes are assured to meet the trust requirements of their sender nodes. If more than one assured route exists, it finds one of the shortest based on number of hops and if all safe routes founded are shortest than the one of the finest suitable is preferred. Again it also has some negative aspects that if nodes do not meet the security requirements then it may drop packets even if the shortest route is available or all links are joined. It picks the first RREP that reaches at the sender. Problem here is that the first RREP comes to the sender may be the false one if there is flooding attack of RREP packets. It does not state anything about how to use the security level as a metric. Route discovery process may lose due to not having appropriate security approval even though there exists a connectivity path to the desired destination. The processing overhead increases on confining flooding mechanism for more optimal and safe routes therefore increasing performance and cost too which is not affordable in low cost networks.

3.3 ARAN

In ARAN [11], there is no assurance that the first route request received travelled along the shortest track from the source. It may be prohibited from travelling on shortest track to reach the destination

because of congestion either legitimately or maliciously. There are certain issues in transmitting ERR messages and in key revocation - It is difficult to find whether the node transmitting bulky ERR messages is compromised or simply out of order. ARAN does not differentiate between these two and looks all irregular behavior as the same. If the trusted certificate server broadcasts an announcement for the revocation of a particular node, to the ad hoc group that wants its revocation. Any node receiving this announcement re-broadcasts it to its neighbors so that they reorganize routing to avoid transmission through the untrusted node. Problem here is that in some cases, the untrusted node that is having its certificate withdrawn may be the only connection between two parts of the Ad hoc network. In this case, the untrusted node may not forward the announcement of revocation for its certificate, causing partition of the network that persists until the untrusted node is no longer the only connection between the two partitions. If an attacker node has attained certificate then ARAN cannot stop fabrication of routing messages. It is protected as long as certificate authority is not compromised. It has high processing overhead and needs extra memory for the storage of certificates and signatures in the packets. There are also some strong points in ARAN which are worth noticing. Because request discovery messages do not have a hop count and messages are signed at each hop, malicious nodes have no chance to redirect traffic. Error messages are also signed; malicious nodes cannot produce fake error messages. Signed error messages provide non-repudiation which verifies authentication of a source node actually sent error message. A node inserting fabricated messages into the network may be debarred from future route controlling.

The route request packet is signed only by the source node with its own private key and route reply packet is signed only by destination node's signature and certificate, this ensures that only the destination can reply to route discovery message. Any modifications in transit would be immediately identified by intermediary nodes along the track, and the modified packet would be consequently discarded. It is effective in finding the shortest routes to the destination in least congested networks.

But infeasible in extremely congested networks because the first route discovery packet reached to the destination may have travelled along the long path due to congestion in the network. Congestion may prevent the discovery of shortest routes but ARAN efforts to pick not only shortest route but also least congested route too.

3.4 ARIDANE

ARIADNE [1] does not consider the case in which an attacker compromises the trusted Key Distribution Centre; if it is compromised then the full network is compromised. It prevents from only one compromised node. An attacker can extend the route by adding extra compromised nodes along the route. This can add delay in the network because nodes like to prefer the shortest route. Route Error message is not processed until the TESLA key gets revealed; this causes delay in knowing that the route is erroneous and in between data packets still continue to be sent along that broken route. In a certain part of network, an attacker intentionally hold Route Requests from a certain node for some period and initiates unnecessary Route discoveries with the chain values from the past discoveries, to make other area nodes believe that it is flooded. Mechanism of key exchange is very complicated. But due to TESLA key's protection, forged route error message cannot be sent. It uses one-way hash function to make sure that no hop is excluded. This is its advantage that any alternation in the node list is detected. If an attacker tries to alter the keys and message authentication code in reply packet, such an alteration is identified due to target MAC field in the reply. Each route request consists of a list of nodes to avoid, and then the message authentication code forming the initial hash chain is computed over that list of nodes.

On spotting suspect in Detecting forged routing messages in Ad hoc networks [12], it broadcasts an alert message to all network nodes except to the suspected node. It then updates its topology table according to the TC message information unless it is verified that the suspected node is an intruder. To decrease the false positives, it applies several checks before declaring a suspected node as an intruder because a node may loses topology information due to collisions and mistakenly alleged a good node as an intruder or attackers may flood fake alert messages to declare good nodes as intruders. A node is declared to be an intruder if at least other n different nodes declared it.

In their work, they have chosen n=2, but the performance increases when n rises. But the problem in this method is that the number of nodes n has a certain threshold. On increasing n, number of false negatives also increases. It is assumed that nodes and message authentication, integrity is already provided and messages cannot be altered in transit. In detection of the node-capture attack in mobile WSN [8], each node flooding n messages every t seconds to show their existence to other nodes. It

is assumed that the message authentication mechanism is already present and a node's memory can only be modified or tampered if it is removed from the network. It requires a fixed threshold of alarms to revoke a node. In simulation, at start, data structure in each node is initialized in a way that it has met all nodes in the set, and without performing attack it is run for 1000 seconds. Due to memory limitation, it is assumed that a maximum of 20 nodes can be traced by each node. Its positive aspects are that the false positive alarms are avoided. It does not require same offset time for the node but accepts skew and drift error [13], [14]. Loose time synchronization can also be considered. Raising MIT doesn't raise number of false positives, but raising alarms reduces number of false positives.

3.5 SRAC

SRAC [15] is not feasible for large network nodes having least resources because if n nodes are present along a path, then it requires generating and allocating (n-1) 2/2 keys to the nodes on the path. Route error messages are not protected. There is large overhead due to encryption/decryption. It is not efficient for low computing nodes because in a large mobile network, links broke more frequently and it has to deal large number of route error messages. It is assumed that a source node and target node cannot be attacked. But it does well in some cases like each node (intermediate) along the route computes the TQI value and passes it to the next hop until it reaches to the target node. The target selects the path by comparing their TQI values and chooses the most efficient with least cost. Only the source node and target node have the authentic keys to decrypt the routing messages. SRAC differs from the basic routing protocol AODV, ARIADNE and ARAN. SRAC holds many paths to the target node whereas AODV holds only one path in its routing table. Therefore, in SRAC, on link breakage, routes are not created again. It just picks up another one.

3.6 HIGH PERFORMANCE FIREWALLS in MANETs

High Performance Firewalls in MANETs [16] has some implementation overhead. It is costly as it requires service specific entries to be maintained in routing table and transmitting of control traffic in the network. Its performance is evaluated for filtering of malicious activity at destinations only. But the good thing about this method is that routing advertisements are only sent to the nodes which are authorized to access that service and packets for a service are only accepted from nodes to which routing advertisements were sent. This scheme can be implemented by any routing protocol with some minor modifications, while being transparent to upper layers and implements packet

filtering by taking advantage of underlying routing mechanisms. It helps to drain battery power of the compromised nodes faster. It is an effective firewall mechanism for highly dynamic networks as it creates boundaries between regions that have different policies, even in changing topology. Therefore, achieves high performance irrespective of the network mobility. It drops unwanted packets very early and further away from the destinations depending on how far ROFL announcements can propagate in the network and saves a lot of battery power. ROFL announcement is stored at each intermediate node because RREP is unicast back to the route initiator along the reverse path that RREQ traversed. Therefore, it doesn't require extra control messages as compared to AODV because client route information is piggy-backed in RREQ messages initiated by the route requestor at the beginning. It reduces control traffic as RREQ packets from unauthorized nodes are dropped silently by neighbors which have seen that ROFL announcement before.

3.7 FrAODV

The effectiveness of FrAODV [17] is that as the number of friends increases, the network performance also increases. Routing message load is less. Their results prove that less control packets need to broadcast in the network because it blocks routing messages traffic from the unreliable nodes. It is a simple method based on evaluating friendship values without any use of encryption/decryption mechanism. And it is not costly. But the weak side of this method is that it accepts any new node's MAC address. E.g. A legitimate node lost its connection for sometime but regains after some time period and joins the network. Its MAC address is not changed but it might become compromised in between by some attacker node. In high mobility network, frequent breakage of links causes generation of RERR messages, removal of broken links and again forming new paths which raises high routing messaging activity. Also RERR messages are not protected. An attacker may produce false RERR messages. It can incur delay in high mobility networks if attackers use the support of RERR messages therefore downs the network's performance.

3.8 TWO LEVEL SECURE RE-ROUTING (TSR)

TSR [18] detects network abnormalities at the transport layer with the help of congestion window (CW) and reacts at the network layer with the help of alternate route finder (ARF). Alert message is authenticated using shared keys and a node cannot produce more than one alert message to prevent from false announcements. Re-routing does not depend upon route error packets. ARF module

checks route history to disable the duplicate suppression in re-routing process. But question arises here is that what if attacker compromises a watch node? then compromised watch node may send false alarm for a good node just to divert the traffic to some other longer route and it may happen that attacker doesn't fabricate the authenticity of alert message so that no other node doubts on it. If compromised nodes are present in large number, they can accuse an honest node to be misbehaving by generating fake alert messages against it one by one. TSR enhances the DSR scheme. In DSR, the source node waits for a route error packet to initiate re-routing whereas in TSR, congestion window surveillance (CWS) module first checks the abnormalities in the network. If detected, then it initiates re-routing. This enables the source to initiate re-routing if route error packets are dropped by some malicious node in the false route.

3.9 ENHANCED AUTHENTICATED ROUTING FOR AD HOC NETWORKS (E-ARAN)

E-ARAN's [19] recommendation process makes it hard for selfish node to create a reputation attack for a certain period. Also its Data acknowledgement (DACK) is signed. But problem with this scheme is that as number of selfish nodes increases, end-to-end delay of data packets also increases because at every hop, each node needs to check its reputation table before forwarding data packets to the highest reputation value next-hop node. Therefore, it also reduces the throughput of network.

3.10 QOS-AWARE ROUTING BASED ON BANDWIDTH ESTIMATION FOR MANET

In [20], we studied two bandwidth estimation schemes which outperform each other in different scenarios. "Hello" bandwidth estimation scheme is better than "Listen" scheme in mobile topologies and has better end-to-end throughput because if route breaks by losing "Hello" messages, then the other flows used the underestimated bandwidth. But in "Listen" scheme, when the route breaks, the node has no knowledge of the bandwidth consumed by each node in the broken link. Therefore it is unable to release the occupied bandwidth immediately which eventually affects the accurate bandwidth estimation. Therefore it slightly drops the end-to-end throughput. In static topologies, both of these schemes perform likewise by using large weight factors which reduces the accidental lost of "Hello" messages that incorrectly signals a broken route and cause congestion. But "Hello" scheme has slightly extra overhead than the "Listen" scheme because it appends "Hello" messages with the information of bandwidth consumed by neighbor node. This method also obscures hidden nodes effect by leaving extra bandwidth for them. It has some more flaws that the overhead caused by the retransmission of RTS, CTS, and ACK packets due to fading errors affect

differently on different size of packets. Therefore, different weight factors are used for different size of packets.

3.11 QoS ENABLED ANT COLONY-BASED MULTIPATH ROUTING FOR MANET

In [21], routes are selected based on path preference probability metric which is computed by next hop availability (NHA) metric. NHA is further computed by taking other metrics that are node availability, link availability, battery life etc. Hop count is another key metric considered for path computations. This protocol incurs additional overhead of control packets for periodically updating the paths and for searching new paths using FANT and BANT messages. So, it has slightly higher overhead as compared to AODV. But it has higher packet delivery ratio than AODV because it also considers other metrics like node stability and link stability. The advantage of using multiple paths and path preference probability is that when source node receives active route failure message due to node mobility, then it at once invalidates that failure link in its routing table and chooses another best valid route from its routing table. This protocol also shows increase in the network's lifetime because nodes with the longest remaining battery time are selected for the construction of long live path from source to destination.

3.12 GATEWAY DISCOVERY ALGORITHM BASED ON MULTIPLE QOS PATH PARAMETERS BETWEEN MOBILE NODE AND GATEWAY NODE

Algorithm [22], has considered path availability time period as an important metric to select a potential gateway between two networks. This metric specifies the total time a MANET node takes to access the gateway node and it is computed by evaluating the minimum link availability period between intermediate nodes along the path between a MANET node and a gateway node. The other metrics used are path latency and residual path load capacity on which different weighting factors are applied for computing overall weight. These weighting factors are application specific and it is claimed that this algorithm even increases throughput in case low weight is assigned to one of the three metrics. Another good approach of this scheme is that it also incorporates feedback mechanism which allows source node to remain intact with the status of the route which makes it more practical and therefore reduces end-to-end delay and congestion.

3.13 BANDWIDTH-SATISFIED MULTICAST TREES IN MANETS

In [23], there is a slight overhead of generating and recovering bandwidth-satisfied multicast tree because it needs additional control information especially in case the number of nodes increases. Authors have evaluated in their results that admission ratio goes lower when multicast groups exceed 5 because it also increases the number of forwarders and therefore extra control packets need to be produced. But as compared to MCEDAR, it performs still better. Moreover, the main strength of this approach is that it removes hidden route and hidden multicast route problems.

3.14 DISTRIBUTED FAULT-TOLERANT QUALITY OF WIRELESS NETWORKS

In [24], the gateway node connecting the two clusters has all information about the routes to the destination node present in one cluster and the source node present in the other cluster. So, redundancy of routing control messages in the network and connection failures also gets reduced. Thus, it reduces the overhead of rerouting from the source node on connection failures. So, it is efficient in connection reestablishments. One more unique feature of this protocol is that when a node allocates its resources, it waits for a certain time period and if it does not get response within that time limit, it de-allocates its resources. Thus, it helps in reserving resources for another flow.

CHAPTER 4

METHODOLOGY

Based upon the literature survey it was observed that different methods and models are available to provide security and QoS in MANETs. However in all the solutions, the focus is towards nullifying attacks or providing QoS. There exists no solution which talks about improving security and QoS simultaneously. So in this model, we propose a system architecture which takes care of QoS and security issues and try to create a secure routing solution. The system architecture for providing QoS and security in MANETs is shown in Figure 3.1. It comprises of Packet Receiver, Packet Forwarder, QoS Routing Module (RM), System Security Module (SSM) and Data Security Module (DSM).

<table>
<tr><td colspan="3">Packet Forwarder</td></tr>
<tr><td>Data Security Model(DSM)
Public Key Cryptography</td><td>Data Security Model(DSM)
Public Key Cryptography</td><td>Data Security Model(DSM)
Data Fragment</td></tr>
<tr><td>System Security Model (SSM) Single path</td><td>System Security Model (SSM) Alternate path</td><td>System Security Model (SSM) Multipathing</td></tr>
<tr><td colspan="3">QoS Routing Model</td></tr>
<tr><td colspan="3">Packet Receiver</td></tr>
</table>

Figure 4.1 Secure QoS Architectural Model

The packet forwarder shown in figure 4.1 relays the packets from one network segment to the other and it uses the entire packet forwarding models like unicasting, multicasting, broadcasting and any casting. It forwards the packets based on the priority assigned by routing module, timestamps the packet before forwarding to the next hop and records the QoS values asked by the source and the assigned values for future updating. It also analyzes the packet based on the values attached to its

header by the lower layer models the packet receiver also is used in the model to receive the packets from the interface. It monitors the interfaces for any error, data loss, checks the type of packet, like the packet is for unicasting, multicasting or broadcasting, and attaches a two bit code for the packet forwarder to understand. It assigns the incoming time stamp to packets and buffers the packets if more packets come in. The QoS model Layer takes care of the QoS and uses any routing protocol preferably the routing protocols with multiple paths and embeds the layered parameters in MANETs. This model also helps in finding the appropriate route between source and destination. It uses a four layered approach. At the physical level it understands the behavior of the neighboring node by checking the node mobility and signal strength of the neighboring node. The control layer does traffic classification and assigns priorities to each class of traffic. Route layer determines shortest path route to the destination, checks for queue level, power level etc. and the application level layer determines delay and throughput in the network. This model provides security at the node level. It does three important functions. It establishes the security solution on to the network, it eliminates the nodes with selfish and malicious behavior and finally it sets up the link with trusted nodes in place of the eliminated nodes. This model takes care of the security at data level. This type of security gets deployed between the source and the destination. The source uses either arithmetic approach or the double split approach to encrypt the data. The data is decoded at the destination with the help of the either the common procedure or with the key which the sender passes to the receiver through separate paths.

4.1 QOS ROUTING MODEL

QoS needs a set of service requirements to be met by the network while transporting a packet stream from source to destination. Many of the proposed QoS routing protocols deal with bandwidth requirement. However we present a model for QoS which identifies various parameters for providing QoS. This model can be applied for any routing algorithms for MANETs however; it works much better for the routing algorithms capable of establishing multiple routes. A node apart from acting as a router and the sender/receiver also becomes capable of informing the best possible route based upon the application demands of the sender node from physical layer to application layer. The model uses four layers. The names of the layers have been given keeping in view the actual wireless communication. The physical layer will deal with the parameters related to 802.11 IEEE physical layers, the control layer talks about 802.11 MAC, the route and application layer takes care of the additional parameters needed in routing and network layer of the OSI model.

$$d = \frac{TR - TL}{2} \times k \tag{1}$$

$$L_s = \begin{cases} 1, & \text{if } d \leq \mu \text{ or } |AP| \leq |AC| \\ 0, & \text{if } d > \mu \text{ or } |AP| > |AC| \end{cases} \tag{2}$$

$$\text{where} \quad |AP| = \sqrt{\alpha^2 + \beta^2} \tag{3}$$

$$|AC| = \sqrt{m^2 + n^2} \tag{4}$$

$$v_{sr} = v \left[\frac{f_e - f_r}{f_r} \right] \tag{5}$$

$$T = \frac{d}{v_{sr}} \tag{6}$$

Given above are some of the mathematical equations that take care of QoS parameters. Eq(1) finds the distance d between nodes and can be found out by the time span from the moment at which a packet starts to occupy the wireless medium to the time at which the immediate acknowledgment is received is measured and denoted by T_R. The time duration between the reception of a data packet and issuing the corresponding immediate acknowledgment is also measured and denoted by T_L. $k = 3 \times 10^8$ m/s is denoted as the speed of light. The position P (α, β) of the neighboring node can be estimated from the distance above. Link stability Ls in terms of distance and position is, given in equation (2) (3)and (4) and μ and C(m, n) are respectively the maximum permissible distance and maximum coordinate position allowed to communicate between the nodes. The node is also capable of finding its energy level by the following equation

$$E_L = C_E - E_C \tag{7}$$

Where C_E is the Consumed energy due to packet transmission and reception and depends on the available power of the node and on the time. E_C is the current energy and E_L is the Energy left. Initially every node has full battery capacity which is assigned to current energy. On each

transmission or reception of a data packet the remaining energy is found using eq (7) and a two bit code is assigned. If the remaining energy falls below 50%, that node will not act as a router to forward the packets will be discarded from the network.

4.2 ENERGY ENHANCEMENT

In this QoS layer, the energy is also enhanced. The proposed algorithm, intends to save energy by using variable transmission power. We have focused on the fact that for efficient and reliable communication/ transfer of data, there is no need for the sender node to transmit data at full transmitting power at all times. Efficient and reliable communication of data can be ensured even at lower transmission powers, provided the intended receiver receives the signal with power above certain threshold value (i.e. receiver sensitivity). Once the route has been established between the end points by the routing protocol, the nodes along the route may have different distances between them, and hence the minimum power required to send data correctly will be different. Here proposed algorithm comes into action and asks the nodes to transmit data to next hop at certain calculated power level (i.e. Optimum Transmission Power) rather than transmitting at default/ maximum transmission power, thereby saving some amount of energy at every hop. In this way, said algorithm provides large scope for energy conservation. To implement the algorithm we need a metric to measure power of the received signals, for this purpose we have used RSSI. AODV protocol has been used in this process. In this the process of route discovery is divided into two phases. In first phase known as the Route Request phase, the source node that needs a valid route to the destination generates an RREQ with all its fields properly initialized and then broadcasts the RREQ. The RREQ generated by the originator is rebroadcasted by the intermediate nodes till it reaches the destination. Once the RREQ packet reaches the destination the second phase i.e. Route Reply Phase comes into action. In this phase, RREP packet generated by the destination is unicasted hop by hop back to the originator node and hence completing the Route Discovery Process. The section below briefly describes the Route Request Phase and Route Reply Phase.

4.2.1 Route Request Phase

The source node initiates the route discovery process by broadcasting the RREQ packets with Total Transmission Power Required initially set to zero. Each node that receives a broadcasted RREQ packet, checks if it has previously received the RREQ with same flooding Id and originator node, if

it has then this node silently ignores the newly received RREQ. If received RREQ has not yet been processed, then the node calculates following parameters.

The Optimum Transmission Power (OTP) value with which they have received the signal;

$$OTP = txPowerdefault – (RSSI – RxSensitivity) + guard$$

The total transmission power required (TtlTxPwrReq) for the path traversed up to that node;

$$TtlTxPwrReq = TtlTxPwrReq + OTP$$

Once the node calculates the OTP and Total Transmission Required, route table entries are made. The two calculated parameters, OTP and Total Transmission Power Required are also stored in the routing table as, OTP for next hop and Total Transmission Power Required respectively along with other fields of the route table entries. Like AODV, the modified energy oriented AODV also stores routes both for the source and the node from which this intermediate node has received the route request. In this way complete reverse path from current node to the originator node is formed at each hop. Then the node currently handling the route request checks if it is the destination, if it's not the destination, then the current node rebroadcasts the RREQ. However Before further forwarding the RREQ packet, the Total Transmission Power Required field of the RREQ packet is modified with the „Total Transmission Power Required calculated at the current node. The process continues till the destination is reached. This forms the complete reverse path along with the values of OTP required from destination node to the originator node. This is the path that will be used to send route reply RREP packet back to originator node

4.2.2 Route Reply Phase

When the RREQ packet reaches the destination, the destination prepares a RREP packet and then following process takes place. Destination checks for the next hop, towards the originator node, from the routing table towards the source and properly initializes the fields of RREP packet with both Transmission Power Required and Total Transmission Power Required initialized to OTP. The destination node unicasts RREP to the next hop towards the originator node.

When a node receives a RREP, it creates a route table entry for the forward route to destination along with the OTP for the hop from which it received the RREP and the Total Transmission Power Required.

If the current node is not the originator node then it fetches the route to the originator node from the route table and makes the corresponding changes in RREP for Transmission Power Required and Total Transmission Power Required as shown below:

$$TxPwrReq = OTP \; TtlTxPwrReq = TtlTxPwrReq + OTP$$

The current node then forwards the modified RREP to the next hop as fetched form the route table. The process continues till the RREP reaches the originator node thereby forming the complete forward path from source to the destination. Once the RREP packet reaches the originator node, and the originator node makes route table entries the route discovery process is complete. Now the source has the complete path to the destination for data transfer and each node has the required OTP value for next hop stored in its routing table.

4.2.3 Data Transmission Phase

When the RREQ packet reaches the destination, the destination prepares a RREP packet and then following process takes place. If an active route to the destination is not available in the routing table, then the node initiates route discovery process. If an active route to the destination is available in the routing table then

1) The node consults the routing table to fetch the next hop for the destination along with the required OTP.
2) The node adjusts the transmission power of its transmitter equal to the OTP.
3) Node starts transmission of the Data to the next hop at the OTP.

When the data reaches any intermediate nodes, the intermediate node again checks its routing table for an active route to the destination and same process is repeated till the data reaches the destination.

4.3 SYSTEM LEVEL SECURITY

The security in MANET is an essential component for routing protocols. MANET operation can be easily jeopardized if countermeasures are not embedded into basic routing protocol functions at the early stages of their design. Unlike infrastructure networks, MANET is formed by a group of mobile nodes connected by wireless links where these nodes can make communication with each other by direct peer-to-peer wireless communication when they are close to each other. When the sender and receiver are far away, their packets can be forwarded by the intermediate nodes along a multi-hop path. The functions of packet routing are carried by all available nodes in the network. Unlike the infrastructure networks, the nodes in Ad hoc network are more difficult to be trusted. This is at the core of the security issues that are specific to mobile Ad hoc networks. The reliability of routing functions can be endangered by any node in wireless mobile Ad hoc network. So thorough checking of the intermediate nodes responsible in route formation is therefore needed. This is achieved through this layer of system level security. In it we have the option of creation of single path, alternate path or multipath monitoring based on the density of the node. The single path is created in such a way so that every node participating in routing process not only forwards packets to destination but also reverses the acknowledgement of packets to the node leaving one hop in between in the reverse route. The alternate path works as per the mathematical equations given below

$$f_{i+1}(f_i(...(n))) = f_{i-1}(f_i(...(n_i, t_i))) \quad (8)$$

For example for a network where the level of nodes are four stage deep, the parameter T1-T4 will be calculated by the source node as mentioned below from the equations. In case any of the below does not hold, we change the route f_i by replacing the corresponding unfit node at corresponding level T_i. The security is further strength- end by using a verification mechanism in the route 1 by getting replies at certain intervals of time from two hop nodes.

T1
$$f_2(f_1(n_{11})) = \bar{f}_1(\bar{f}_2(n_{12}, t_2)) \quad (9)$$

T2
$$f_3(f_2(f_1(n_{12}))) = \bar{f}_1(\bar{f}_2(\bar{f}_3(n_{13}, t_2))) \quad (10)$$

T3
$$f_4(f_3(f_2(f_1(n_{14})))) = \bar{f}_1(\bar{f}_2(\bar{f}_3(\bar{f}_4(n_{15}, t_2)))) \quad (11)$$

T4

$$f_5(f_4(f_3(f_2(f_1(n_{15}))) = \overline{f}_1(\overline{f}_2(\overline{f}_3(\overline{f}_4(\overline{f}_5(n_{16}, t_2))))) \quad (12)$$

Multipathing is created initially by checking the route replies received and if the formations of multipath are possible then data is sent along those paths. Initially multi paths are preferred because of many reasons like, load balancing, delay reduction etc but if the creations of multiple paths are not possible then the single or alternate path is created. In multipathing the data is fragmented as a message can be divided into N pieces called shares. In order to compromise the message, the adversary must compromise at least the minimum threshold number of shares required to reconstruct the message. With fewer than threshold number of shares, the attacker cannot learn anything about the message and has no better chance to recover the secret.

4.4 DATA LEVEL SECURITY

Route monitoring is not enough as the trust value of the monitoring node cannot be ascertained and moreover the intruders can get the data from the network and use it for malicious purpose. In order to provide additional layer of security, the data level security is provided. In this approach, any public key cryptographic system is used to create the additional layer of security at the data level from source to destination. The famous RSA algorithm is used. The system layer security proposes three ways of route selection based on the density of the nodes. The multipath routing is always proposed as in this there is no requirement of node or path monitoring because the data in data layer security fragments the data based on the principles of visual cryptography. However if the system layer selects either alternate path or single path then public key cryptosystem is uses to secure the data.

4.5 SECURE QOS ROUTING

The above parameters identified in QoS layer along with the routing path determination is applied to any routing protocol already existing for MANETs preferably capable of creating multipaths.

R.No	SID	DES	INID*	RID	BW	BL
1	S	D	1,2,3,4	1	11,10,11	11,10,11,10
2	S	D	5,6,7,8,9	1	11,10,11	11,11,10,10,11
3	S	D	1,5,3,4	1	11,01,11 ,11	11,10,10,10
4	S	D	1,5,6,8,9	1	11,11,11 ,11,10,1	11,11,11,11,10 ,11

Table 1: Route Adoption Stage

4.5.1 Route Discovery Phase

As mentioned above, we can use either single path to provide QoS and security but our protocol first will try to find multiple paths to destination then select, single path, alternate path or multipath to forward data in a secure fashion and provide QoS as well. The source node S as shown in Figure 1 when needs to send data to destination D, it initiates a route discovery process and broadcasts a route request packet (RREQ), which contains the following information like source address(SA), destination address(DA), request id(RID) and also contains the QoS parameter information like battery life (BL), bandwidth (BW), stable time link(STL) with the neighboring node. It is assumed that the node has the capability to calculate the distance and frequency as per the equations given above and also to find the link stability duration. Each route request (RREQ) also contains a record listing the address of each intermediate node through which this particular copy of the RREQ message has been forwarded. The nodes which receive the RREQ, checks the DA, SA and RID. If it matches with its own DA, it returns a route reply (RREP) message to the initiator of the route discovery otherwise it forwards the packet.

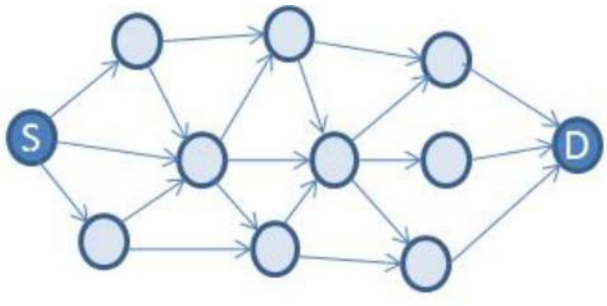

Figure 4.2: Route Request Initiated

In reply to the RREQ, the destination checks the route and sends back the reply to the source or else checks its cache for an already existent route. The source then caches this route in its route cache for use in sending subsequent packets to this destination, otherwise, the intermediate node attaches its own address to the RREQ and broadcasts it to its neighbors. This process continues till the destination is arrived. It may happen that the intermediate node may get repeated RREQ's through various neighbors. The Intermediate node then checks the request id and the intermediate node id list (INID). If the similarity is found in the request id or an entry is in the address list, the packet is rejected else the packet is selected for forwarding and the address of the node is added to the address list if no route exists in the cache. The source on the receipt of the RREP packet back from destination forms the source route.

4.5.2 Route Adoption Stage

The RID is the route number, SID the source address, DESID is the destination address, INID is the intermediate node numbers, RID the route request packet no. BW the bandwidth available and finally the BL represent the Battery life available. Once the source gets the RREP from its neighboring nodes and forms the source table, it checks all the entries and takes decision about main route formation based on bandwidth, battery life entry. The two bit entry in the table specifies the bandwidth and the battery level available. The 11 indicates full (100-75) %, 10 as (74-50) %, 01 as (49-25) % and 00(24-5) %. The purpose of doing this is to discourage nodes having less bandwidth and battery life by not including them in the route formation as less bandwidth and battery life changes the node behavior from normal to selfish. The route adoption stage uses one more route to monitor the activities of main route. This is formed in such a way so that every node on the main route is heard by the other nodes participating in main route check. Once the main route and check route is formed, the data is sent through main route and security check processes are activated either single path monitoring, alternate path monitoring or data fragmentation using multipathing monitoring.

CHAPTER 5

RESULTS & ANALYSIS

The Simulations has been done first to check the performance enhancement of already existing Routing Protocol AODV in terms of its energy enhancement in nodes. The above purposed algorithm has been given here the name of rOTP-AODV just to make out the difference between our approach and the already existing AODV. The results have been simulated in Qualnet 5.1. We have compared its performance with AODV. Various simulations have been carried out to analyze the working of rOTP-AODV. Simulations have been performed with static nodes as well as mobile nodes. The section below describes the simulation environment used and various associated parameters.

5.1 SCENARIO 1

Here we have considered an Ad hoc Network having 20 static nodes (Figure 5.1) and rOTP-AODV as its routing protocol. Table below shows the parameters and their values.

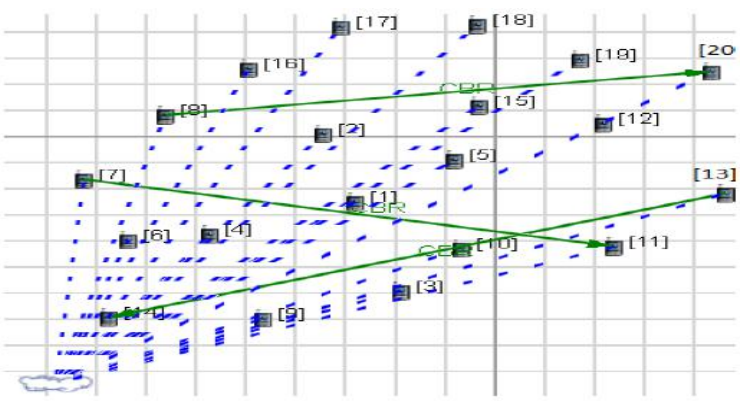

Figure 5.1 Screen Shot of Scenario 1

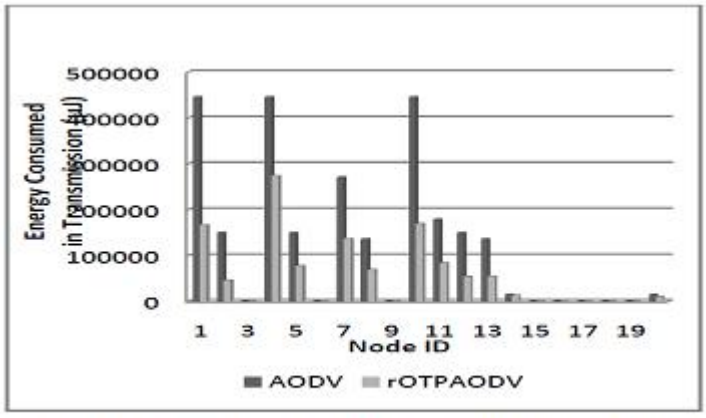

Figure 5.2 Comparison of energy consumed by nodes using AODV and rOTP-AODV

Figure 5.2 presents the comparison of energy consumed in transmission by nodes when using AODV and rOTP-AODV as routing protocol. From the chart it is evident that huge amount of energy is being saved when rOTP-AODV is used as compared to AODV. However it can also be noticed that the energy consumed by proposed algorithm rOTP-AODV is more than AODV if the number of data packets transmitted by the node is less than the number of control packets sent by same node. Further it may be understood that for same number of control packets to be transmitted, rOTP-AODV consumes more energy in transmission than AODV as the size of these control packets in rOTP-AODV is more than in AODV

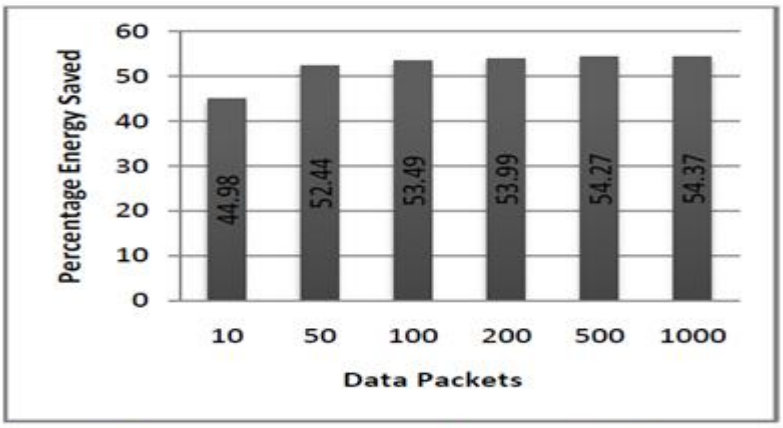

Figure5.3 Percentage energy saved V/s no. of Data Packets (for each CBR)

The effect of number of data packets to be transmitted on the energy savings attained by rOTP-AODV has also been analyzed. Figure 5.3 presents the percentage of energy saved by rOTP-AODV when compared to the energy consumed by AODV routing protocol. The simulation results show that rOTP-AODV can save energy around 50%. The simulation results also show that the percentage of energy saved increases with the increase in number of data packets sent over the CBR links.

5.2 SCENARIO 2

When we talk about wireless Ad hoc networks, mobility is one of the main features. Hence it becomes important to investigate the performance of rOTP-AODV in a network with mobile nodes. The nodes in scenario 2 obey random waypoint mobility. Other parameters associated with the simulation environment are shown in the table below.

TABLE II
Parameters Of Scenario 2

Parameter	Value
Simulator	Qualnet 5.1
No. of nodes	20
Simulation Time	200s
Environment Size	1500 x 1500 m^2
Transmission Power (Default)	20 dBm
Receiver Sensitivity	-85 dBm
Traffic Type	CBR (Constant Bit Rate)
Packet Size	512 b
Packet Rate	10 packets/s
Mobility model	Random Way Point
Speed	1m/s
Pause Time	2s
Antenna Type	Omni directional

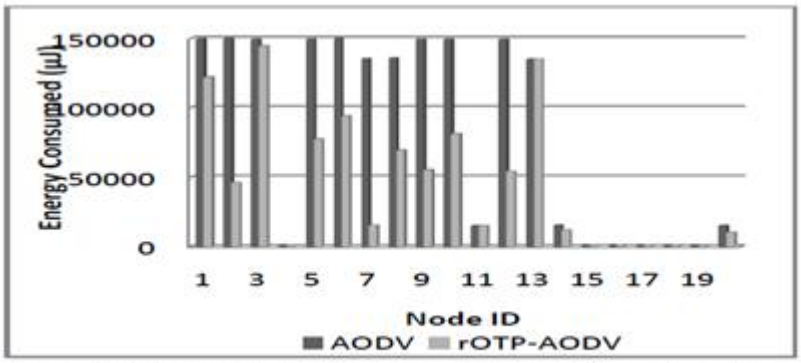

Figure5.4 Comparison of energy consumed by nodes using AODV & rOTP-AODV (Scenario 2)

Figure 5.4 presents the comparison of energy consumed in transmission by nodes when using AODV and rOTP-AODV as routing protocol for scenario 2. In the current simulation environment 43% of energy is saved network wide. However when compared with energy saving in network with static

nodes energy saving has reduced. This is because of the increased number of control packets flowing through the network owing to the link breakages caused by mobility. To complete the comparison between AODV and rOTP-AODV it is necessary that we analyze both the protocols on other quality of service indicators as well. In the section bellow we have compared AODV and rOTP-AODV on the basis of Throughput, End-To-End Delay, and Jitter.

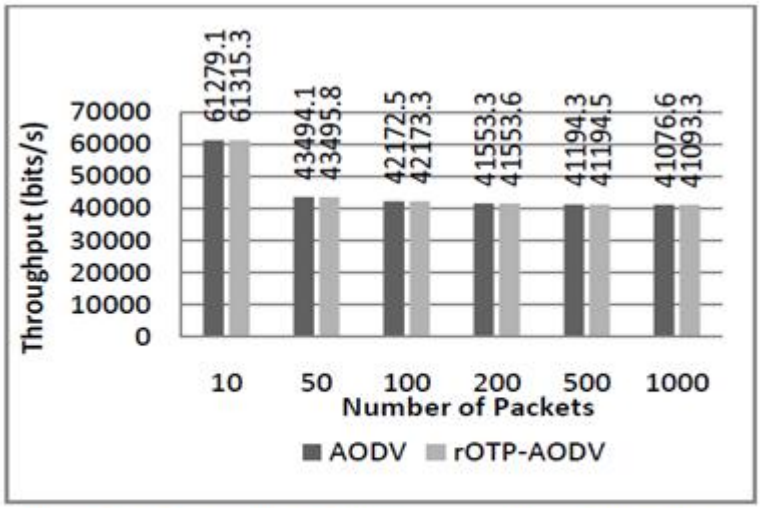

Figure 5.5 Comparison of throughput observed at nodes using AODV & rOTP-AODV

Figure 5.5 depicts the comparison of throughput versus number of packets generated by each CBR when using AODV and rOTP-AODV as their routing protocol. It is quite evident that there is no adverse effect of rOTP-AODV on throughput, instead throughput has increased marginally.

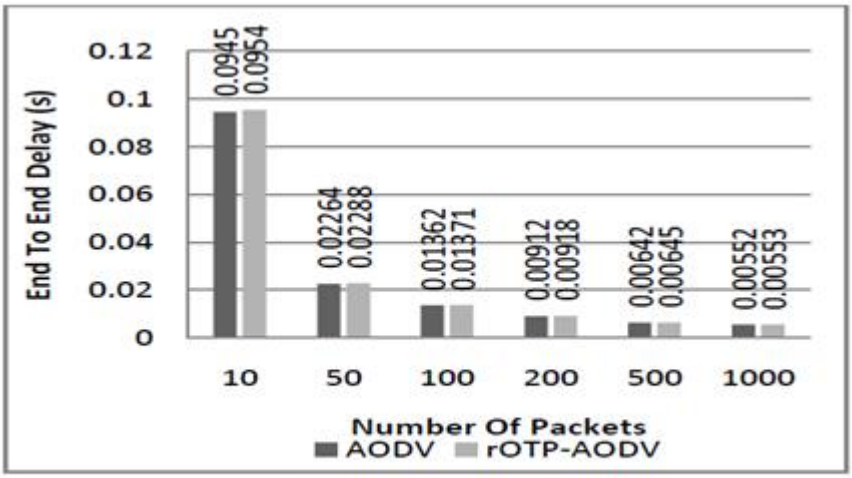

Figure 5.6 Comparison of End to End Delay observed at nodes using AODV & rOTP-AODV

Figure 5.6 presents the comparison of AODV and rOTP-AODV on the basis of End to End Delay. Simulation results show that End To End delay has marginally increased (0.6 %) when rOTP-AODV was used. However such small increment in delay can be ignored in lieu of significant amount of energy consumed in transmission of data that can be saved by using rOTP-AODV.

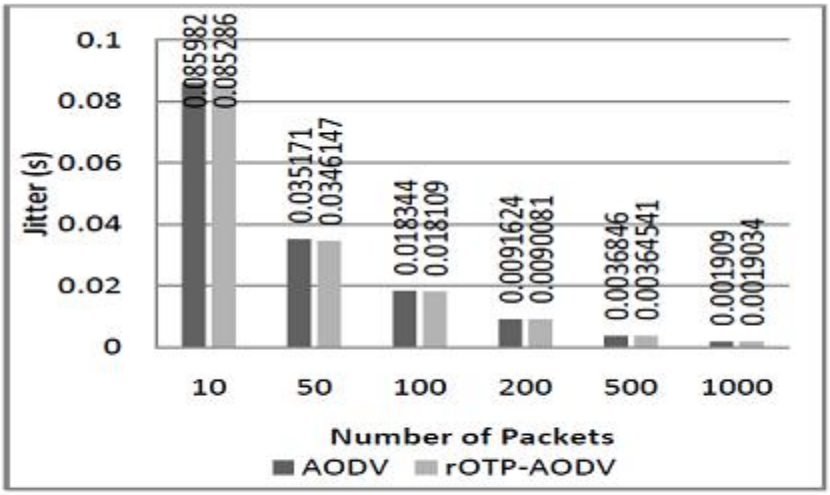

Figure 5.7 Comparison of Jitter observed at nodes using AODV & rOTP-AODV

Figure 5.7 shows the comparison of AODV and rOTP-AODV on the basis of Jitter. As can be seen from the above figure, the jitter has slightly reduced (1.1%) when we used rOTP-AODV as routing protocol.

The proposed routing algorithm rOTP-AODV is an energy efficient algorithm which tries to conserve as much energy as possible while transmitting data between end points. The rOTP-AODV after route discovery process transmits data at optimum transmission power which each node has calculated and stored in routing table during route discovery process. By transmitting data at OTP considerable amount of energy can be saved. Simulation results have shown that for wireless Ad hoc networks with static nodes as much as 50% of energy consumed in transmission can be saved thereby considerably extending the network lifetime. The amount of energy saved also increases as the number of data packets flowing through the network increases. However simulation results have shown and also justified our assumption that for rOTP-AODV to be effective the number of data packets should be very large compared to the control packets. Simulation results have also shown that for Mobile Ad-hoc networks the energy saved by rOTP-AODV is around 40%. And the amount of energy saved in MANETs is bound to decrease with increase in mobility. The decrease in energy saved is due to the increased number of link breakages, which lead to more number of control packets flowing through the

network. Simulation results have also shown that rOTP-AODV does not adversely effects other major quality of service parameters such as Throughput, End to End Delay, and Jitter. In fact, except for End to End Delay which increased marginally (0.6%) both other parameters Throughput and Jitter have improved with the use of rOTP-AODV over AODV. So we can say that proposed Algorithm i.e. rOTP-AODV performs better than AODV.

5.3 SCENARIO 3

The identified parameters will be incorporated all in future and the protocol will be modified accordingly. However we are using some of the parameter evaluation on AODV and AOMDV protocols to check their performance. The proposed method is also used with the low density to high density of nodes in the network and accordingly single, alternate or multipath are selected. We have calculated the packet delivery ratio to destination and network throughput to ensure the dedicated quality of service.

Parameter	Value
Simulator	Qualnet 5.1
Area	1500x1500 m^2
Number of Nodes	90 (30,60,90)
Simulation Time	900 s
Traffic Type	CBR (Constant Bit Rate)
Packet Size	512 Bytes
Bandwidth	2Mbps
Frequency	2.4Ghz
Routing Protocol	AODV
Mobility Model	Random Waypoint
Pause Time	0s
Maximum Speed	0-20 m/s

Table 3: Parameters of Scenario 3

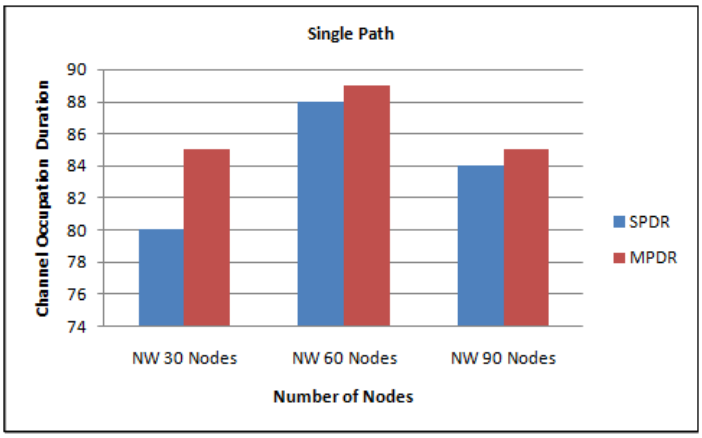

Figure 5.8 Comparison of Packet Delivery Ratio (PDR) during Single path monitoring

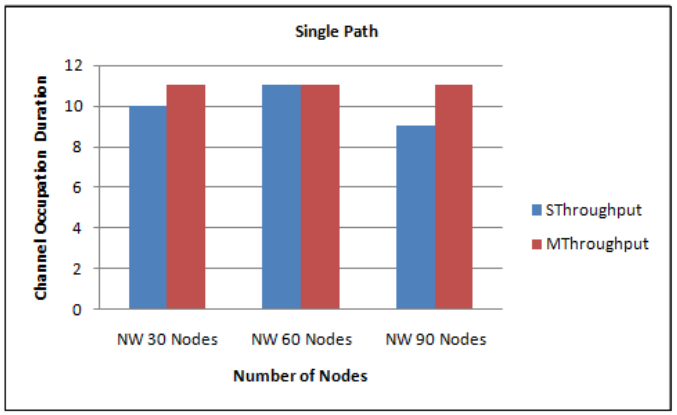

Figure 5.9 Comparison of Network Throughput during Single path monitoring

The figure 5.8 depicts the general case of packet delivery ratio with different values of standard AODV and modified approach using Single path. Figure 5.9 shows the network throughput performance during single path monitoring.

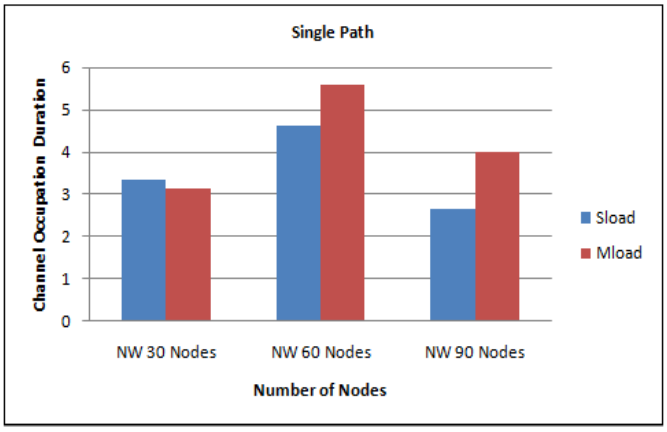

Figure 5.10 Comparison of Routing Load during Single path monitoring

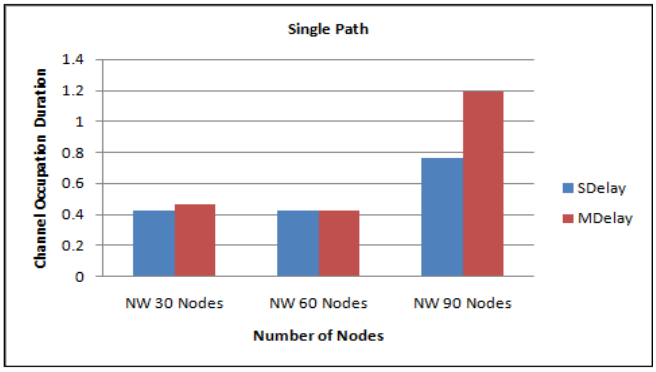

Figure 5. 11 Comparison of End to End Delay during Single path monitoring

Figure 5.10 depicts Routing Load and Figure 5.11 represents the End to End delay with different values of standard AODV and modified approach using Single path Monitoring. We compare the performance of protocols with three cases of network size from low density to high density (Network with 30 nodes, Network with 60 nodes and Network with 90 nodes).

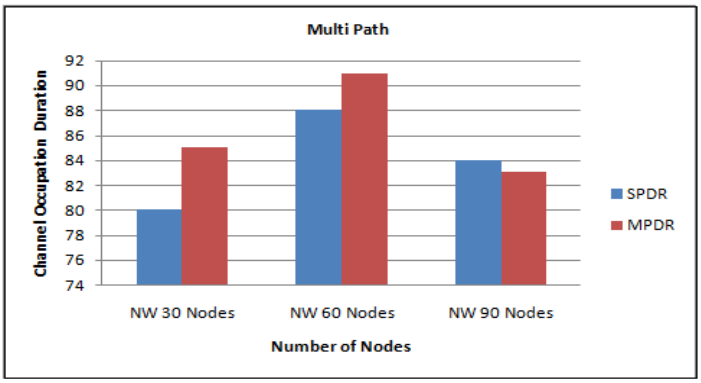

Figure 5.12 Comparison of Packet Delivery Ratio (PDR) during Multipath monitoring

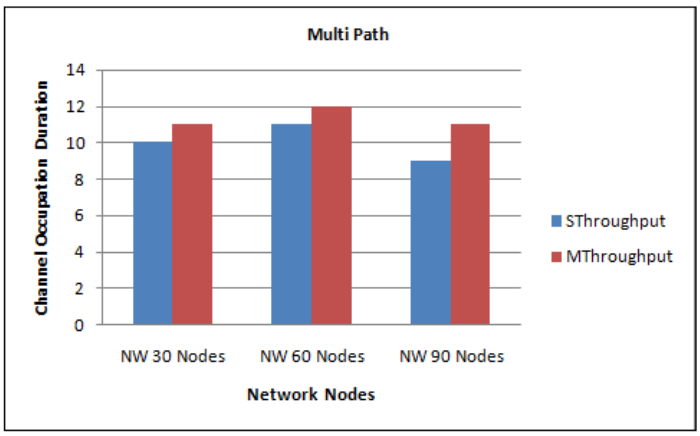

Figure 5.13 Comparison of Network Throughput during Multipath monitoring

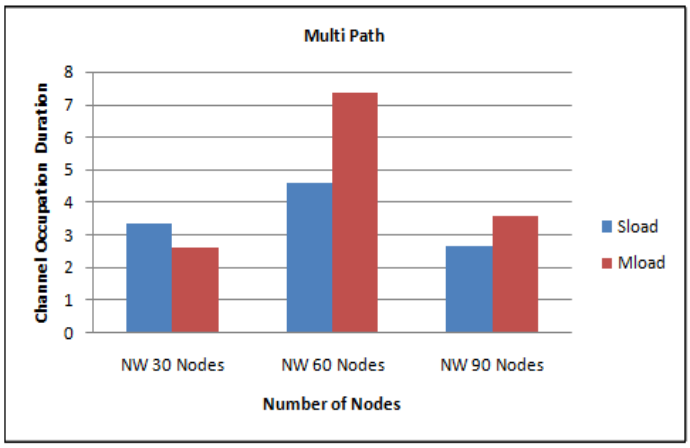

Figure 5.14 Comparison of Routing Load during Multipath monitoring

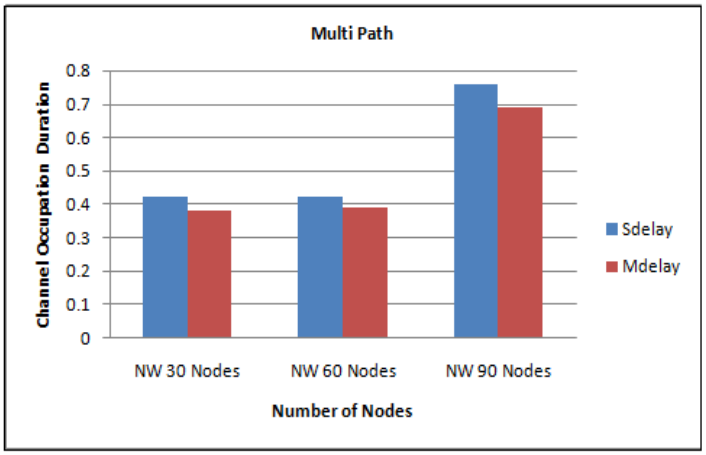

Figure 5.15 Comparison of End to End Delay during Multipath monitoring

The figure 5.12 shows the calculation of packet delivery ratio with different values of standard AODV and modified approach using Multipath monitoring. The figure 5.13 represents network throughput, figure 5.14 depicts routing load as well as figure 5.15 shows the end to end delay with different values of standard AODV and modified approach using Multipath monitoring. We compare the performance of protocols with three cases of network size from low density to high density.

REFERENCES

[1] Y.C. HU, A. Perrig, and D. B. Johnson, "ARIADNE: a secure on-demand routing protocol for Ad hoc networks," in *Proc. MOBICOM,* 2002, pp. 12-23.

[2] P. Papadimitratos and Z. Haas, "Secure routing for mobile Ad hoc networks," in *Proc. CNDS,* 2002.

[3] Y.-C. HU, A. Perrig, and D.B. Johnson, "PACKET LEASHES: a defense against wormhole attacks in wireless networks," in *Proc. INFOCOM,* 2003, pp.1976-1986.

[4] Y.-C. HU, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless Ad hoc network routing protocols," in *Proc. WISE,* 2003, pp. 30-40.

[5] J. F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems," in *Proc. Wksp. Design Issues in Anonymity and Unobservability, Berkeley, CA*, 2000, pp. 7-26.

[6] J. Hubaux and E. W. Knightly, "Denial of service resilience in Ad hoc networks," in *Proc. MOBICOM*, 2004, pp. 202-215

[7] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Emergent properties: Detection of the node-capture attack in mobile wireless sensor networks", ACM WiSec, 2008 pages 214-219.

[8] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. "A performance comparison of multi-hop wireless Ad hoc network routing protocols" in *Proc. MOBICOM*, 1998, pages 85–97.

[9] S. Marti, T. Giuli, k. Lai, and M. Baker, "Mitigating routing misbehavior in mobile Ad hoc networks," in *Proc. MOBICOM*, 2000, pp. 255-265.

[10] S. Yi, P. Naldurg, and R. Kravets, "A Security-Aware Routing Protocol for Wireless Ad hoc Networks", in *Proc. MOBIHOC*, 2002 pp. 286-292.

[11] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields and E. M. Belding-Royer, "A Secure Routing Protocol for Ad hoc Networks," in *Proc. ICNP* , 2002, pp. 78–87.

[12] A. Fourati; K. Al Agha, "Detecting forged routing messages in adhoc networks", Springer published on nov, 2008, pp.205 – 214.

[13] S. Ganeriwal, S. Capkun, C. C. Han and M. B. Srivastava. Secure time synchronization service for sensor networks. In WiSe, 2005, pages 97–106.

[14] K. Sun, P. Ning, and C. Wang, "Fault-tolerant cluster-wise clock synchronization for wireless sensor networks" TDSC, 2005, pg.177–189.

[15] S. Albert Rabara and S.Vijayalakshmi, "Rushing attack mitigation in multicast manet (RAM3)", in *Proc, IJRRCS*, 2010, pp. 131-138.

[16] H. Zhao and S. M. Bellovin, "High Performance Firewalls in MANETs" *Proc. MSN*, 2010 pages 154-160.

[17] T. Eissa; S. A. Razak; R. H. Khokhar; N. Samian, "Trust-Based Routing Mechanism in MANET: Design and Implementation", Springer, Mobile Networks and Applications June 2011.

[18] H. N. Saha, D. Bhattacharyya, A. K. Bandhyopadhyay and P. K. Banerjee, "Two-Level Secure Re-routing (TSR) in Mobile Ad hoc Networks" *Proc. MNCAPPS*, 2012 Pages 119-122.

[19] A. Jangra, Shalini, N. Goel, "e-ARAN: Enhanced Authenticated Routing for Ad hoc Networks to handle Selfish Nodes" *Proc. ICAESM*, 2012 pages 144-149.

[20] L. Chen and W. B. Heinzelman, "QoS-Aware Routing Based on Bandwidth Estimation for Mobile Ad hoc Networks", IEEE Journal on SAC, 2005, pp. 561-572.

[21] P. V. Krishna, V. Saritha, G. Vedha, A. Bhiwal, A.S. Chawla, "Quality-of-service-enabled ant colony-based multipath routing for mobile Ad hoc networks", Commun, IET, 2012, pp. 76- 83.

[22] S. H. Bouk, I. Sasase, S. H. Ahmed, and N. Javaid, "Gateway Discovery Algorithm Based on Multiple QoS Path Parameters Between Mobile Node and Gateway Node", IEEE JCN, 2012, pp. 434 – 442.

[23] C. -C. Hu, E. -H. Kuang Wu and G.-Huey Chen, "Bandwidth-Satisfied Multicast Trees in MANETs", IEEE Transactions On Mobile Computing, 2008, pp. 712-723.

[24] L. C. Llewellyn, K. M. Hopkinson and S. R. Graham, "Distributed Fault-Tolerant Quality of Wireless Networks", IEEE Transactions On Mobile Computing, 2011, pp. 175-190.

List of Publications

1. Ajay Koul, Mamta Bucha, "Cumulative Techniques for Overcoming Security Threats in Manets", International Journal of Computer Networks and Information Security, Vol 5 2015, pp 61-73, DOI: 10.5815/ijcnis.2015.05.08

2. Ajay Koul, Harinder Kour, "Quality of Service Oriented Secure Routing Model for Mobile Ad hoc Networks", Proc. Of International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence, March 25 - 27, 2017, ACM, Hong Kong., 2017.