Secure Routing Environment with Enhancing QoS in Mobile Ad-Hoc Networks

Gautam M. Borkar
Department of Computer Engineering
RGIT, Versoval Andheri(w) Mumabi 53
gautam.borkar@mctrgit.ac.in

Anjali R. Mahajan
Department of Information Technology
Government Polytechnic College, Nagpur Maharashtra.
armahajan@rediffmail.com

Abstract: A mobile adhoc network is infrastructure-free and self configured network connected without wire. As it is infrastructure-free and no centralized control, such type of network are suitable only for conditional inter communication link. So initially maintaining Quality of Service and security aware routing is a difficult task. The main purpose of QoS aware routing is to find an optimal secure route from source to destination which will satisfy two or more QoS constrain. In this paper, we propose a net based multicasting routing scheme to discovery all possible secure path using Secure closest spot trust certification protocol (SCSTC) and the optimal link path is derived from Dolphin Echolocation algorithm (DEA). The numerical result and performance analysis clearly describe that our provided proposal routing protocol generates better packet delivery ratio, decreases packet delay reduces overhead in secured environment.

Keywords: *Mobile adhoc network (MANET); Multicasting routing scheme MRS; Quality of Service ; Secure closest spot trust certification protocol (SCSTC); Dolphin Echolocation Algorithm (DEA).*

*****

I. Introduction

Mobile adhoc network is system composed of wireless mobile nodes that creates temporary connection among them self to enable communication without proper communication infrastructure. In such network topology mobile nodes can communicate directly with all mobile nodes with radio range [1, 2] whereas some nodes that are not in directly in communication range uses intermediate nodes to communicate with each other [3]. All the mobile nodes that had participated in transfer data from source to destination forms a wireless therefore such topology can be viewed as MANET [4]. Routing protocol for MANET must compact with restriction such as high error rate, scalability, security, quality of service, energy efficiency, multicast, aggregation and node cooperative etc. Here, qualitative properties like security and quality of service are taken into description.

Earlier research assumed a friendly and cooperative environment and focused on problem such as wireless channel access and multi hope routing, security has become major concern in due course of time in order to provide protected communication between the nodes in potentially hostile environment [5].

QoS generally defined as service requirement that consider the parameter of network to be fulfilled while transporting the data packet from source to destination [6]. QoS routing not only finds a path from source to destination, but also a route that fulfils QoS parameters such as end-to-end delay. But while going for QoS, early study security has not been consider. Without adequate security unauthorised access and usage may go against QoS, so we need to design secure aware routing. On other hand if we go for secure aware routing, such as authentication, confidentiality, integrity and availability overhead will be increased which will indirectly affect QoS. Here some study is required which will provide improved QoS in secure environment.

The main technical contribution of our work are summarised as follow.

1. We derive trust and definition firstly, then abstract of multipath routing model, where the trust entity those who are interested neighbour form basis network topology for this model. On the bases of interested entity historical behaviour multi dimensional trust attribute are incorporate to respect trust relationship in various side.
2. The standard ad hoc on demand multi-path distance vector protocol is increased as basic algorithm to calculate security and trust based multipath routing model. For secure and trust multipath routing, no of hop count, secure forward path trust and secure reverse path trust, this three matrix calm a three dimensional assessment is done for routing decision and Dolphin Echolocation (DE) algorithm gives a flexible and feasible route to generate multiple both-way associative trust path, by neglecting un trusted nodes for finding the shortest path.
3. The implementation evaluation shows that the given multipath routing scheme provides much better result

in attack prevention and increases the QoS such as packet delivery ratio, end-to-end delay etc.

The remaining paper is organised as follows. Second section discusses the related work. In third section we introduce secure closest sport trust certification (SCSTC) protocol in detail. In forth section analysis and result is given. And finally section five concluding remark of the paper.

II. Related work

B. Paramasivanet al. [7] have used the random Bayesian signalling game to study the concept profile for normal and malicious nodes in MANET for Routing. This game also showed the best achievement of individual strategies for every node. Perfect Bayesian equilibrium (PBE) gives a appropriate answer for signalling games to solve deficient data by integrate strategies and payoff of players that initiate equilibrium. In big networks, it gives more overrun cluster framework which increases the routing overhead so, they proposed Ad hoc on demand Distance Vector (AODV) provides reliable data transmission in MANETs. In AODV, there was a requested source and destination sequence number, which is the essential reason for the routing loop problem and for privacy. This approach minimizes the utility of malicious nodes and it motivates better cooperation between nodes by using the reputation system. Regular nodes monitor continuously to evaluate their neighbors using belief updating systems of the Bayes rule. Even though the regular nodes are follow the PBE strategy to reduce the malicious node utilities for improving throughput in the entire networks. The performance analysis concludes that the PBE strategy was the best strategy for regular nodes to reduce malicious nodes utility. In this analysis, throughput and routing latency are about 91% respectively, than other protocols that improve the networks performance.

HaiyingShenet al. [8] have proposed a QoS-Oriented Distributed routing protocol (QOD) to enhance the QoS support capability of hybrid networks. Taking advantage of fewer transmission hops and any cast transmission features of the hybrid networks, QOD transforms the packet routing problem to a resource scheduling problem. QOD incorporates five algorithms:- QoS-guaranteed neighbor selection algorithm to meet the transmission delay requirement, Distributed packet scheduling algorithm to further reduce transmission delay, A mobility-based segment resizing algorithm that adaptively adjusts segment size according to node mobility in order to reduce transmission time, A traffic redundant elimination algorithm to increase the transmission throughput, A data redundancy elimination based transmission algorithm to eliminate the redundant data to further improve the transmission QoS. A number of queuing scheduling algorithms have proposed for Differentiated Service (DiffServ) to further minimize packet droppings and bandwidth consumption. Analytical results based on the random way-point model and the real human mobility model show that QOD can provide high QoS performance in terms of overhead, transmission delay, mobility-resilience and scalability. The traffic redundant elimination based transmission algorithm can further increase the transmission throughput. In the future they placed to evaluate the performance of QOD based on the real tested.

Wei Liu et al. [9] have proposed a new routing protocol is Authenticated Anonymous Secure Routing (AASR), to satisfy the requirement and defend the attacks. More specifically, the route request packets are authenticated by a group signature to defend the potential active attacks without unveiling the node identities. The key encrypted onion routing with a route secret verification message, was designed to prevent intermediate nodes from inferring a real destination and also check whether AASR can achieve the anonymity goals by three anonymities namely identity anonymity, route anonymity, and location anonymity. To develop the anonymous protocols, a direct method is to anonymize the commonly used on-demand ad hoc routing protocols, such as AODV and ANODR. These results were used to compare the performance of AASR to that of ANODR, in a representative on-demand anonymous routing protocol. The results show that, it provides more throughput than ANODR under the packet-dropping attacks, although AASR experiences more cryptographic operation delay. Compared to ANODR, AASR provides higher throughput and lower packets loss ratio in different mobile scenarios in the presence of adversary attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio. In future, they will improve AASR to reduce the packet delay. A possible method was to combine it with a trust based routing. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks.

Yang Qin et al. [10] have proposed a novel statistical traffic pattern discovery system (STARS). STARS aims to derive the source and destination probability distribution, i.e., the probability for each node to be a message source and destination, and the end-to-end link probability distribution, which is the probability for each pair of nodes to be an end-to-end communication pair. To achieve its goals, STARS includes two major steps one is to Construct point-to-point traffic matrices using the time-slicing technique, and then derive the end-to-end traffic matrix with a set of traffic filtering rules, and next one is Apply a heuristic approach to identify the actual source and destination nodes, and then correlate the source nodes with their corresponding destinations, which use the probability distributions produced by STARS are good indicators of the actual traffic patterns, i.e., actual sources, destinations, and end-to-end links. and which reveals most of the actual end-to end links by slightly sacrificing the false-positive rate. Specifically, in most cases, more than 80 percent of the actual end-to-end links are revealed (i.e., the false-negative rate was less than 0.2), while the false-positive rate was not more than 0.16.

Xu Li et al. [11] analyze the impact of network load on MAODV protocol, and proposed an optimized protocol MAODV-BB (Multicast Ad hoc On-demand Vector with Backup Branches), which improves robustness of the MAODV protocol by combining advantages of the tree structure and the mesh structure. The extension of MAODV protocol was to construct a multicast tree with backup branches from two aspects. One is the process of backup branches selection and addition, the other is the mechanism of multicast tree maintenance. It not only can update shorter tree branches but also construct a multicast tree with backup branches. As a tree based multicast routing protocol, MAODV-BB shows an excellent performance in light weight ad hoc networks. Mathematical analysis and this result both demonstrate that the MAODV-BB protocol improves the network performance over conventional MAODV in heavy load ad hoc networks. MAODV-BB's packet delivery was always maintained at a high level even when the network load is heavy also obvious to see that the delay of MAODV-BB is always lower than MAODV's.In MAODV-BB, the existence of backup branches reduces the frequency of tree reconstruction and ensures high packet delivery ratio in heavy load ad hoc networks.

III. MESH BASED MULTICAST ROUTING IN MOBILE ADHOC NETWORK

The group-oriented services are one of the primary application by Mobile Ad hoc Networks (MANETs) in recent years. To support such services, multicast routing is used. Thus, there is a need to design stable, reliable and secured multicast routing protocols for MANETs to ensure better packet delivery ratio, lower delays, reduce overheads and security mechanism handles misbehaviors and avoid various attacks. To overcome the above problems occurred in MANET, A mesh based multicast routing scheme will proposed in this work.

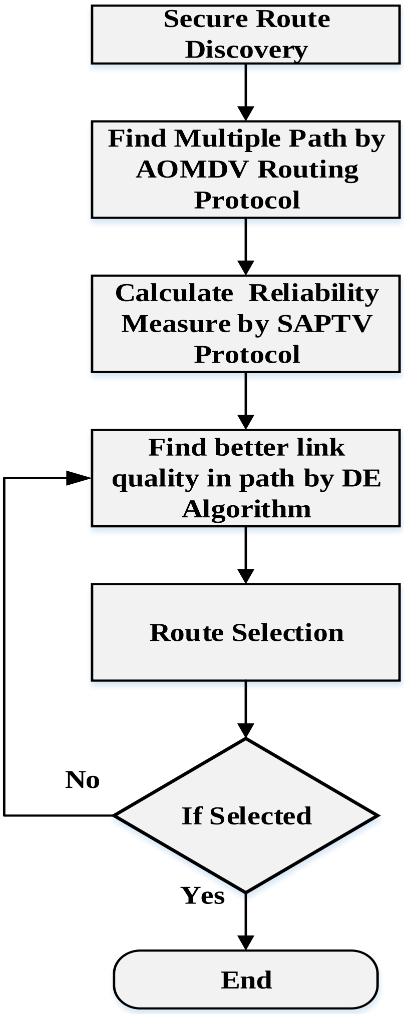
Secure Route Discovery
Find Multiple Path by AOMDV Routing Protocol
Calculate Reliability Measure by SAPTV Protocol
Find better link quality in path by DE Algorithm
Route Selection
No
If Selected
Yes
End

Figure.1 Proposed Flow diagram

The proposed multicast routing scheme (MRS) finds stable multicast path for multimedia transmission in MANET. A multicast mesh is constructed and the transmission route will discover in two stages. In first stage to maintain the quality of routing the physical parameter analysis will done by analyzing Transmit Energy, Distance, channel load, buffer occupancy, bandwidth and bit error rate (BER). Then in second stage the security of route will analyze by using route request, Erroneous Report Detection (ERD) scheme and route reply packets. One of the most stable paths with better quality for routing in the secure environment is discovered by employing ant colony optimization (ACO) technique. Then the Route maintenance will process to maintain the routing in case of any link failure happened. The proposed scheme is simulated over a large number of MANET nodes with wide range of mobility and the performance is evaluated. The performance of the proposed scheme is compared with the existing routing protocols.

IV. Find Better Link Quality Optimal Path Using DE Algorithm for Data Transmission

An optimization technique called DEA is used to find better link quality path to transfer data into our proposed network scheme. DEA can be applied to optimization problems that are partially in dynamic topology changing environment. DEA is applied to find the best nodes involved in a path. DEA is meta-heuristic that searches large spaces of candidate solutions. A route with a better link quality is selected for forwarding data from source to destination. If a better link quality is not found, DEA function is performed again until global best solution has been found. DEA reduces the traffic and routing overhead of the optimization process and finds the node with best link quality in an ad hoc network.

DE Algorithm for optimal route selection

The main steps of dolphin echolocation (DE) for discrete optimization are as follows:

Initialize nodes (number of echolocations) in a MANET.

For echolocation i, this is at distance (i)

Initialize the Secure routes with a uniformly distributed random vector (u_1, u_2)

$$V = W * v + y_1 * u_1 * (p - x) + y_2 * u_2 * (g - x)$$

This update uses a weighted sum of the following:
(i) The previous velocity V is found by speed packet
(ii) The difference between the current distance and the best distance the particle has seen $(p - x)$
(iii) The difference between the current distance and the best distance in the current

```
DE Algorithm
Step 1: (Initialization):
Set $u_1 = 0$;
Set $u_2 = 0$;
Set $V_0 \leftarrow Velocity\ of\ packet\ speed$;
Set $Q_0 \leftarrow \arg\min v(v_0)$
Start the routing process at the initial state $L_0$;
Step 2(Find Accumulative fitness for possible routes)
    for $u_1$ =1tothe number of Routes
    for $u_2$ =1tothe number of variables
    find the position of L $(u_1, u_2)$in j-th column of the
    Alternatives matrix and name it as A.
    for $u_3$ =-Reto Re
    $AF_{(A+u_3)u_2} = \frac{1}{\mathrm{Re}} * (\mathrm{Re} - |u_3|) Fitness(u_1) + AF_{(A+u_3)u_2}$
Step 3 (Find the best route):
    For $u_2$ =1: Number of variables
     for $u_1$ =1:Number of alternative routes
     If $u_1$ =The best route ($u_2$)
     $AF_{u_1,u_2} = 0$
    End
```

DEA is initialized with a group of secure paths and then searches for an optimal route solution by updating generations. Each echolocation is updated by two best values in the iterations. The first one is the best solution that has been achieved previously. The second best value is tracked by the dolphin rules obtained currently by any paths in the population. The bound of the inertial range option is use for providing a satisfactory solution that eventually is discovered. This best value is a global best. The DE algorithm significantly reduces the traffic overhead and computation complexity. The DEA reduced the route failure between nodes that minimize the routing overhead. To decrease the effect of random error, every experiment repeats 50 times and the average of experimental results is used as the performance metrics.

V. Results and Analysis

The parameters like throughput, transmit energy, channel load, buffer occupancy, transmit distance, bit error rate and packet delivery ratio are improved as previously noted.

Table 4 Parameter analysis Vs Number of nodes

Parameters	No of node	TP (kb/s)	ETD (ms)	TE (J)	BER (%)	CL (%)	BO (%)	PDR (%)
Basic AODV output	20	295	20.3	1580	25.2	21.9	22.8	91.7
	40	614	21.7	3285	20.8	23.1	20.9	92.3
	60	925	22.6	4982	16	17.5	17.1	93.9
	80	1246	23.7	6642	12.8	19.8	15	94.5
	100	1561	24.6	8370	9.1	21.9	12.8	95
Basic	20	286	20.9	1695	30.8	30.5	29	87.2

AODV with attack	40	603	22.5	3385	27.6	26.9	26.1	88.3
	60	914	23.2	5085	24.3	18.9	24	89.6
	80	1235	24.5	6764	18	22.1	22.2	91
	100	1552	25.5	8479	14.7	24	19.1	92.9
AODV with attack prevention	20	300	20.1	1490	23.3	23.3	20.1	93
	40	618	21	3140	17.5	21.9	18.6	94.5
	60	935	21.9	4874	13.9	16.9	15.7	95.2
	80	1254	23	6502	10.7	17.5	13.4	96
	100	1571	23.8	8208	7.1	14.9	11	96.9
AODV with attack prevention but changes in overhead	20	305	19.2	1395	20.5	24.7	18	94.1
	40	624	20	3032	15.4	19	16.1	95.3
	60	942	20.9	4710	11.2	16.1	12.9	96.1
	80	1261	22.1	6410	8.9	13.9	11.2	96.9
	100	1579	23	8102	6.1	11.1	9	98.1
Improved AODV with attack prevention but improvement in overhead	20	317	18.3	1210	15.6	20.5	14.9	95
	40	637	19.1	2954	12.3	17.4	11.8	96.2
	60	956	20	4603	8.8	14.2	9.7	97
	80	1275	21.2	6309	6.3	11	6.8	98.2
	100	1593	22	8001	5	8.3	5	99.1

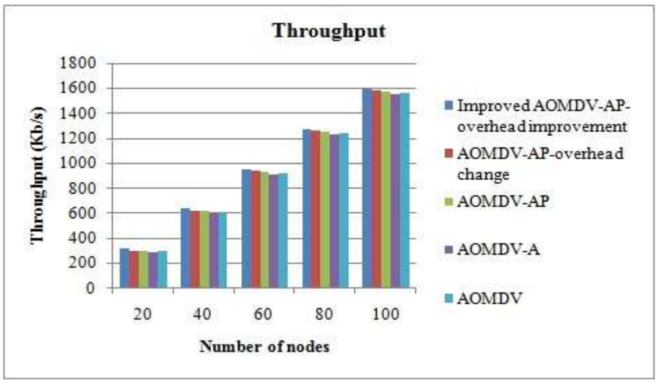

Figure 2: Measurement of Throughput varying maximum number of nodes(Kb/s)

Figure 2 illustrates a comparison among basic AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention),AOMDV-AP-overhead change(AOMDV with Attack Prevention(changes in overhead) and Improved AOMDV-AP-overhead improvement(Proposed AOMDV-SAPTV) in terms of throughput based on random mobility scenario by varying maximum number of connections (number of nodes). The numbers of connections were varied as 20,40,60,80,100 nodes respectively. At high density like from 100 numbers of connections in Improved AOMDV-AP-overhead improvement (Proposed AOMDV-SAPTV), the throughput increases because of packet lost is too low.

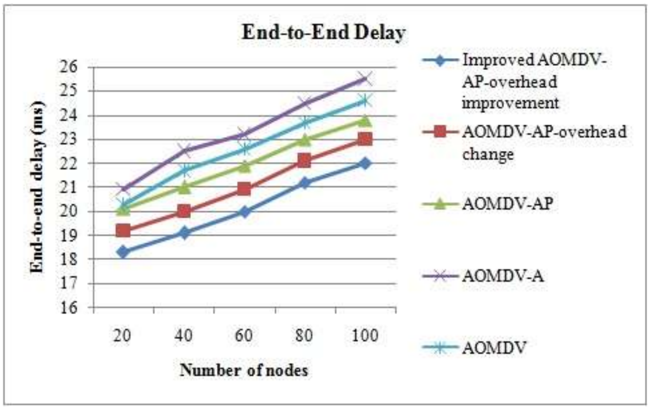

Figure 3: Measurement of End to End delay varying maximum number of nodes (ms)

Figure 3 shows that the average end-to-end delay of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention),AOMDV-AP-overhead change(AOMDV with Attack Prevention(changes in overhead) and Improved AOMDV-AP-overhead improvement(Proposed AOMDV-SAPTV).The average end-to-end delay increases with the increased number of connections. The numbers of connections were varied as 20,40,60,80,100 nodes. After increasing number of connections more than 40, end-to-end delay increase much higher because of queuing and retransmission delay. In heavy traffics load as the maximum number of connections increase, the number of packets delivery also increase. But based on the above graph comparison end to end delay for our proposed AOMDV-SAPTV is very low.

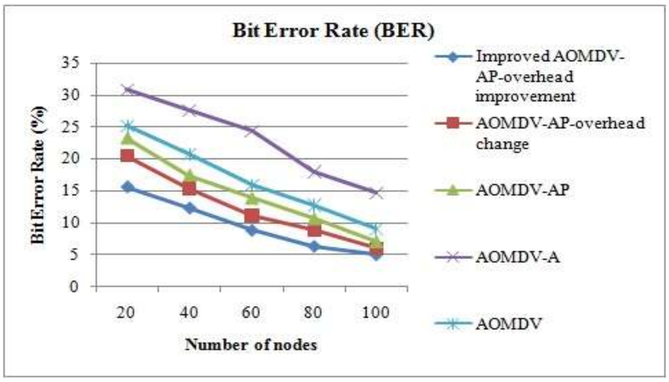

Figure 4: Measurement of Bit Error Rate varying maximum number of nodes

Figure 4 shows Bit Error Rate of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV-SAPTV).Above graph comparison shows Bit Error rate is too low for our proposed AOMDV-SAPTV protocol because of high low packet loss.

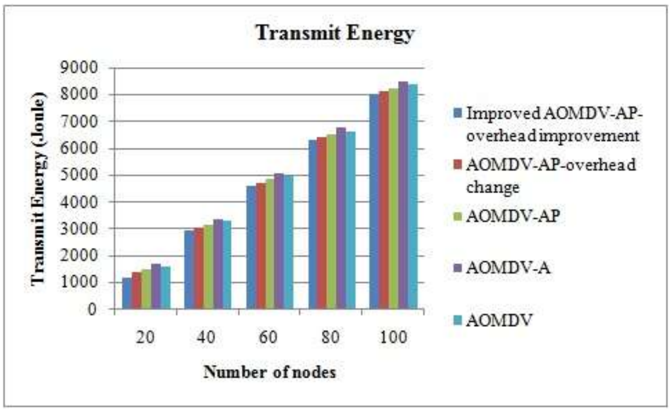

Figure 5: Measurement of Transmission Energy varying maximum number of nodes (Joule)

Figure 5 shows transmission energy of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV-SAPTV) and the maximum number of connections energy consumption respectively. Based on the above graph comparison shows that our proposed protocol AOMDV-SAPTV consumes low energy compared to others. The life time (battery) of the node for AOMDV-SAPTV is higher than other protocol. In the case of a link failure, AOMDV-SAPTV has the ability to make longer battery and node's life time because of the proper utilization in choosing a path.

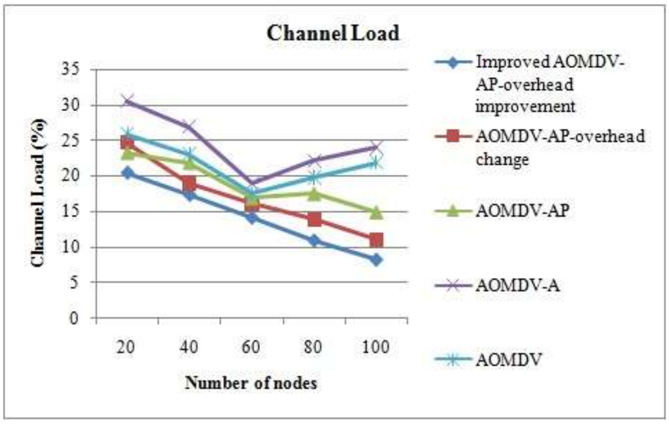

Figure 6: Measurement of Channel Load varying maximum number of nodes

Figure 6 shows channel load percentage of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV-SAPTV).Above graph comparison shows channel load percentage is too low for our proposed AOMDV-SAPTV protocol because of traffic occurrence level is very low.

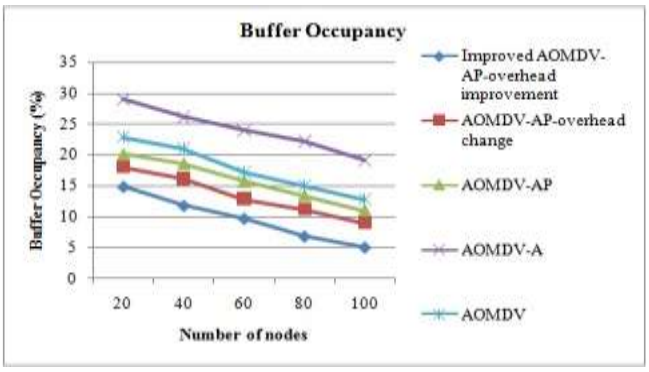

Figure 7: Measurement of Buffer Occupancy varying maximum number of nodes

Figure 7 indicates the effect of buffer occupancy of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV-SAPTV).Above graph shows the proposed routing protocol AOMDV-SAPV using the multipath but congestion avoiding ability of proposed protocol gives better throughput then the AOMDV. AOMDV-SAPTV uses the buffer space of the neighboring node so packet drop is less as compared to the AOMDV. So it shows that AOMDV-SAPTV is better than AOMDV.

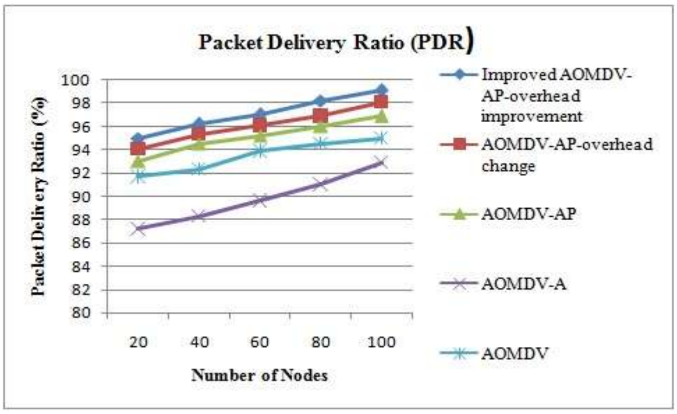

Figure 8: Measurement of Packet delivery ratio varying maximum number of nodes

Figure 8 shows packet delivery ratio of Basic AOMDV, AOMDV-A (AOMDV with Attack), AOMDV-AP (AOMDV with Attack Prevention), AOMDV-AP-overhead change (AOMDV with Attack Prevention (changes in overhead) and Improved AOMDV-AP-overhead improvement (Proposed AOMDV-SAPTV).Above graph comparison shows PDR rate is too high for our proposed AOMDV-SAPTV protocol because of secure trust based optimal route selection.

Based on the above parametric matrices like throughput, transmit energy, channel load, buffer occupancy, transmit distance, bit error rate and packet delivery ratio are improved compared to other existing routing protocols. It denotes our proposed AOMDV-SAPTV provides better QoS (Quality of service) and security against vulnerabilities.

VI. CONCLUSION

Mobile ad hoc networks have attracted much interest in the research community due to their potential applications. However, the inherent characteristics of such networks make them vulnerable to a wide variety of attacks. The security concerned in these wireless networks remains a serious impediment to widespread adoption. In this paper, we focus on the security of routing protocol in MANETs. Firstly, we abstract a secure adjacent position trust verification model. Then by extending the standard Ad hoc On-demand Multi-path Distance Vector protocol (AOMDV), we propose a novel secure adjacent trust-enhanced routing protocol combined with the trust model, named as AOMDV-SAPTV. The persuasive experiments have been conducted to simulate and present the effectiveness of this new protocol.The main purpose of QoS aware routing is to find a feasible path from source to destination which will satisfy two or more end to end QoS constrains. The DE algorithm is used to find the optimal and best path for routing. The proposed scheme is compared to the existing routing protocols. The result shows that our proposed technique enhanced the quality of routing and had find the best path by the optimization algorithm.

REFERENCE

[1] Attar A., Tang H., Vasilakos A. V., Yu F. R., & Leung V. (2012). A survey of security challenges in cognitive radio networks: Solutions and future research directions. Proceedings of the IEEE, 12(100), 3172–3186.

[2] Cordasco J. & Wetzel S. (2008). Cryptographic versus trust based methods for MANET routing security. Electronic Notes in Theoretical Computer Science, 197(2), 131–140.

[3] Azedine B., El-Khatiba K., Xua L., & Korbab L. (2005). An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks. Computer Communications, 28(10), 1193–1203.

[4] Li Wenjia, & Joshi Anupam. (2008). Security issues in mobile ad hoc networks—A survey (pp. 1–23). Baltimore County: Department of Computer Science and Electrical Engineering, University of Maryland.

[5] Yang Hao, Haiyun Luo, Fan Ye, Songwu Lu, & Zhang Lixia. (2004). Security in mobile ad hoc networks: Challenges and solutions. Wireless Communications, IEEE, 11(1), 38–47.

[6] Chunxue Wu, Fengna Zhang and Hongming Yang, “A Novel QoS Multipath Path Routing in MANET”, International Journal of Digital Content Technology and its Applications, Vol. 4, No. 3, pp.132-136, June 2010.

[7] B. Paramasivan, M.J.V. Prakash, and M. Kaliappan, "Development of a secure routing protocol using game theory model in mobile ad hoc networks", IEEE Journal of Communications and Networks, Vol. 17, No. 1, pp. 75-83, 2015.

[8] Haiying Shen and Ze Li, "A QoS-Oriented Distributed Routing Protocol for Hybrid Wireless Networks,", IEEE Transactions on Mobile Computing, Vol. 13, No. 3, pp.693-708, 2014.

[9] Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Vol. 63, No. 9, pp.4585-4593, 2014

[10] Yang Qin, Dijiang Huang and Bing Li, "STARS: A Statistical Traffic Pattern Discovery System for MANETs", IEEE Transactions on Dependable and Secure Computing, Vol. 11, No. 2, pp.181-192, 2014

[11] Xu Li, Tianjiao Liu, Ying Liu and Yan Tang, "Optimized multicast routing algorithm based on tree structure in MANETs", China Communications, Vol. 11, No. 2, pp.90-99, 2014.