Journal of Advances and Scholarly Researches in Allied Education
Vol. XV, Issue No. 1, April-2018, ISSN 2230-7540

Secure & Reliable Routing using Mobility Prediction Algorithm for Mobile Ad Hoc Networks

Satav Sandip Dattatraya[1]* Dr. Avnish Raj Verma[2]

[1] PhD Student, Maharishi University of Information Technology, Lucknow

[2] PhD Guide, Maharishi University of Information Technology, Lucknow

Abstract – With the expanding utilization of wireless networks like Mobile Ad Hoc Networks (MANET) in everyday life, its security prerequisites and protection saving necessities become a significant research challenge. The security of such networks is, for the most part, accomplished with the utilization of security and protection routing protocols. In any case, the vast majority of the protocols are neglected to accomplish both efficient client authentication and secure communication while accomplishing the quality of service (QoS) necessities of wireless networks. In wandering services, attackers may attempt to access different services in wireless networks. Consequently, it's required to have security saving client authentication convention for wireless mobile communications. This can be accomplished by an ongoing Efficient Authentication algorithm (EAA), for all intents and purposes this convention demonstrating the efficient exhibition of security safeguarding and client authentication as far as time and overhead parameters. For wireless networks, alongside protection conservation, secure communication technique planning is additionally a difficult errand. In this manner in proposed work, a Secure and Reliable Routing using Mobility Prediction (SRRMP) algorithm is design and executed which depends on an ongoing EAA convention. SRRMP intended to exhibit efficient client authentication services as well as the reliability of routing convention alongside a security-based mobility prediction algorithm. SRRMP accomplishes two objectives initially is secure routing communication in the system so as to shield against security dangers in a wireless system and second is evaluating the mobility-based path determination to chooses the more steady path. This paper introduced a reliable and secure routing using a mobility prediction conspires for the ad-hoc wireless system: SRRMP routing convention. In SRRMP model, the issue of choosing a reliable path in a mobile ad-hoc system is figured as a bi-goal to secure communication issue dependent on security and mobility prediction measurements. The practical results showing thatthe proposed SRRMP strategy accomplishing the improved QoS execution under various types of attackers in wireless networks.

Keywords: Secure Routing, Mobility Prediction, Mobile Ad Hoc Networks, Quality of Services (QoS).

----------X----------

I. INTRODUCTION

The Ad Hoc networks are configured without infrastructure or centralized controller, which inferences that a node in the network can act as a source or intermediate router or destination node. These types of networks are also commonly recorded as mesh networks because the topology of the network looks like a mesh. The multi communication paths provided by ad hoc mesh networks radically improve the fault tolerance of the network. Additionally, the data packets can hop from one mobile to another mobile that effectively extends the network coverage area and gives a way to overcome Line Of Sight (LOS) issues. The second type, Mobile Ad Hoc network has many additional disputes as changes to the network topology are swift and extensive. The communication routes should be updated quickly and accurately. The MANET can be completely self-contained; it can also be tied to an Internet Protocol (IP) based global or local network.

The MANET nodes are stirred with wireless transmitters and receivers using aerials and antennas that may be unidirectional, bi-directional or some combination thereof. These types of networks are outlined based upon nodes positions, nodes coverage range, transmission power levels and co-channel interference as noise as described by Adarbah et al (2012). At a given point in time, wireless connectivity in the form of a random, multi-hop graph or Ad Hoc network exists between the

nodes. The following are a list of general characteristics of MANET.

1) Dynamic topologies: Nodes are liberated to move in any direction and the topology is dynamic. The nodes move randomly times and nodes consist of both bi-directional and unidirectional links.

2) Limited Bandwidth: Wireless links are having radically lower bandwidth than wired links. In addition, the throughput of wireless links is very much less than a maximum transmission rate of a radio channel because of the effects of multiple access, fading, noise and interference conditions.

In section II, we present a brief review of secure and reliable routing methods applying mobility prediction algorithm for mobile ad hoc networks. In section III, the proposed methodology discussed. In section IV, the simulation results and discussions presented. In section V, conclusion and future work suggested.

II. RELATED WORKS

MANET routing protocols stand measures to be tracked by each defeated hub over pleasingly discovers perfect ways and course bundles between endpoints (source and objective nods). Strong MANET routing protocols strive to create the surviving of the routing approach supporting the closeness of non-routing strategy under the closeness of non - accommodating nodes. In this section, we take a brief review of conventional and recent routing methods.

In [2] Authors presented the managed-open scenario where no network infrastructure was pre-deployed, but a small amount of prior security coordination was expected. The protocol, authenticated routing for ad hoc networks (ARAN), was based on certificates and successfully defeats all identified attacks for secure routing protocol for ad hoc networks.

In [3] developed a hybrid algorithm combining PSO and noising method for solving the shortest path problem in networks. A cost priority-based particle encoding/decoding scheme is proposed in order to incorporate specific heuristic information of the network in the path construction process. The results revealed that this method is found to improve the overall network performance and reduce the computational effort when compared to the standard PSO even for more number of trials and population size.

The Signal Noise Ratio [4] aware routing algorithm: a cross-layer design for MANET. Routing in MANET is complex due to the fact that the network graph is episodically connected and nodes get only intermittently connected because of nodes mobility, terrain, weather, and jamming that change topology rapidly. The proposed cross-layer design is to achieve reliable data transmission in MANET. A key challenge is to create a mechanism that can provide good delivery performance and high quality of service in intermittent networks. The key components include a Cross-Layer Design (CLD) to improve information sharing between different protocol layers. In order to improve the end to end performance of MANET, it is presented a mechanism that allows the network layer to adjust its routing protocol dynamically based on SNR and Received Power along the end to end routing path for each transmission link.

In [5] Siva Kumar and Mahalingam (2011) proposed the complete secure routing protocol is APALLS (Ariadne with Pairwise Authentication and Link Layer Signatures), in view of DSR. APALLS is the primary strong routing protocol that is needed to provide a non-repudiable attestation of dynamic attacks. The first DSR protocol is certainly expected that all nodes will submit to the guidelines. The nearness of nodes that don't hold fast to the guidelines, either intentionally, or because of failing, can deleteriously affect the MANET subnet.

In [7] Author has proposed a new routing method called Link Quality Based Ant Routing Algorithm (LQARA) for MANETs. Swarm intelligence based routing is very suitable for ad hoc networks, regarding its distributed fashion to treat and resolve complex problems using an analogy to a biological swarm of insects. To enhance the ARA routing algorithm, they have defined new metrics to handle the link quality between nodes to evaluate route. The performances of the proposed algorithm are compared to AODV.

In [8], The Deployment of multimedia applications warrants provisioning of Quality of Service (QoS) in MANET. However, limited battery power, other resource constraints and mobility of nodes make QoS provisioning difficult to achieve in MANET. This difficulty can be overcome by using a cross-layer approach (Ruchita et a1 2011) for routing.

In [9], MANET has a random topology with possible additions and deletions of nodes. Each node should continuously sense the neighborhood for topology changes. The strength of the neighbor discovery scheme determines the extent of routing (Dillingham 2007). In [10] Zhang et al (2011) proposed a secure scheme to enable the neighboring nodes to discover each other with maximum probability in the presence of omnipresent jammers, especially for a hostile environment. A scanning based direct discovery algorithm to discover neighbors is presented in the literature with high trust levels (Devi & Thilagavathy 2013).

In [11] author has proposed a Link availability prediction-based reliable routing for MANETs. It considers unpredictable topology changes and frequent link failure into account. The link availability is predicted over a short period of time by estimating

the distance between two adjacent nodes. They have derived an analytical expression for link availability based on the relative mobility of the nodes.

In [12], Han & Lee (2013) proposed an adaptive hello messaging scheme for neighbor discovery that is found to reduce energy consumption and network overhead and promising throughput.

In [13][14], Cornejo et al (2009, 2014) have proposed a layered architecture model with reliable neighbor discovery layer which establishes links such that the packet delivery is guaranteed. Secure neighborhood selection scheme is proposed by Thakre & Kadam (2014) which is able to withstand various security attacks.

In this manner, in section III presented the proposed methodology, an SRRMP algorithm are designed and implemented which depends on an ongoing EAA convention and Mobility Prediction Algorithm discussed.

III. METHODOLOGY

3.1 Parameters in Consideration

To provide a comparison among different authentication and security methods, the following parameters are considered for any wireless network. Some of them are exclusive to the construction or the maintenance processes

- A number of active nodes: This metric measures the quality of the selection policy for nodes. Also, the amount of active nodes selected by the algorithm has a direct impact on the lifetime of the network.
- A number of messages: This metric shows the overhead of the protocol regarding message complexity, which is also related to the scalability of the protocol and the energy consumption.
- The ratio of energy spent: This metric shows the cost of the protocol regarding energy; in other words, how much energy is spent in the execution of the protocol.
- The ratio of the covered area: This ratio is important for comparing coverage-oriented protocols to compare the effectiveness of their selection policies.
- Network lifetime: This metric is useful especially in comparing topology maintenance Protocols, and shows the behavior of some of the previously mentioned metrics in the time domain, to obtain an average behavior of the use of the resources in the network in the long run.

The evaluation of secure routing protocols will be performed in different scenarios, to obtain a general idea of the behavior of the protocols under certain conditions. The list of factors that were used to define the different scenarios is the following:

- A number of nodes: This parameter determines the size of the topology. The variation of this parameter helps to determine the scalability of the protocols. The network sizes used in the experiments will be varied based on the evaluated metric, from very small topologies with only 20 nodes, to very dense topologies with 100 nodes.
- The side of the area L: This parameter defines the size of the deployment area. The area is assumed to be a square of side L. This factor varied between 50 and 2000 meters, depending on the definition of each particular experiment.
- Communication range Rc: This parameter is very useful because it has an implication in other parameters like average node degree. The levels of this factor were calculated mostly using the Critical Transmission Range (CTR) formula. The CTR is the minimal radius that produces a connected topology given the size of the network and the area side L.
- Sensing range Rs: This parameter is important determining the area of coverage of a single node. The levels of this factor are statically defined as a certain ratio of the side of the area L.
- Node location distribution: The distribution of the nodes in the area plays a very important role in the performance of the protocols. Even though many assume uniformly random distribution, some require specific densities in every section of the deployment area.
- Network load: Some messages that every active node will be sent during the operation of the network. This could be constant and periodic or could be variable depending on the occurrence of an event. All experiments assumed a network load of 1 message every 10 seconds per active node.
- Packet size: All experiments use two different message sizes: short messages, assumed to be control packets of 25 Bytes long, and long messages, assumed to be data or special long control packets of 512 Bytes long.

- Initial energy: This parameter represents the initial energy reserve that a node has at the beginning of the simulation. The value assumed for this parameter is 1 Joule per node, as in. This value is considerably small compared with the real amount of energy in the battery; however, it will be selected for convenience to reduce the simulation time.
- Node Mobility: This is another parameter which is vital in deciding the efficiency of load balancing protocol. For this research, we are varying mobility speed between 10 to 50 m/s.
- Number of Attackers: This parameter is used to check the number of attackers in the network. The attackers may vary from 1 to 20 attackers in the network.

Module 1: Implementation and Evaluation of APALLS and ARAN Protocols

Security Routing Protocols: APALLS and ARAN

Number of wireless nodes: 50

MAC: 802.11

Simulation Time: 30 Seconds

Scenario 1: Varying Mobility

Mobility Speed: 5, 10, 15, 20, 25 (m/s)

Number of Attacks: 2

Results Measurement

Throughput vs. Mobility Speed

Loss Ratio vs. Mobility Speed

Overhead vs. Mobility Speed

Delay (Time) vs. Mobility Speed

Scenario 2: Varying Number of Attacks

Mobility Speed: 5 (m/s)

Number of Attacks: 1, 3, 5, 7, 9

Results Measurement

Throughput vs. Varying Number of Attacks

Loss Ratio vs. Varying Number of Attacks

Overhead vs. Varying Number of Attacks

Delay (Time) vs. Varying Number of Attacks

Module 2: Implementation of EAA Protocol and Evaluation against APALLS and ARAN

Security Routing Protocols: **EAA**

Number of wireless nodes: 50

MAC: 802.11

Simulation Time: 30 Seconds

Scenario 1: Varying Mobility

Mobility Speed: 5, 10, 15, 20, 25 (m/s)

Number of Attacks: 2

Results Measurement

Throughput vs. Mobility Speed

Loss Ratio vs. Mobility Speed

Overhead vs. Mobility Speed

Delay (Time) vs. Mobility Speed

Scenario 2: Varying Number of Attacks

Mobility Speed: 5 (m/s)

Number of Attacks: 1, 3, 5, 7, 9

Results Measurement

Throughput vs. Varying Number of Attacks

Loss Ratio vs. Varying Number of Attacks

Overhead vs. Varying Number of Attacks

Delay (Time) vs. Varying Number of Attacks

Module 3: Implementation of SRRMP Protocol and Evaluation against APALLS, ARAN and EAA

Security Routing Protocols: **EAA**

Number of wireless nodes: 50

MAC: 802.11

Simulation Time: 30 Seconds

Scenario 1: Varying Mobility

Mobility Speed: 5, 10, 15, 20, 25 (m/s)

Number of Attacks: 2

Results Measurement

Throughput vs. Mobility Speed

Loss Ratio vs. Mobility Speed

Overhead vs. Mobility Speed

Delay (Time) vs. Mobility Speed

Scenario 2: Varying Number of Attacks

Mobility Speed: 5 (m/s)

Number of Attacks: 1, 3, 5, 7, 9

Results Measurement

Throughput vs. Varying Number of Attacks

Loss Ratio vs. Varying Number of Attacks

Overhead vs. Varying Number of Attacks

Delay (Time) vs. Varying Number of Attacks

3.2 SRRMP Design

In this scenario, we are first presenting the design of proposed Efficient Authentication Algorithm (EAA) method of wireless networks privacy preservation and universal authentication methods under the real-time MANETs with the objective of analyzing the performance and limitations. And then to address the mobility, we present the mobility prediction algorithm. By considering both this Module we formed the proposed SRRMP.

Algorithm 1: Security Algorithm

Step 1: VLR-GS. Keygen (N, $\mathcal{T}$)

1.1 The group manager randomly selects a generator $g \in G$ and $\tilde{g} \in RG$. Additionally, it selects $hj \in RG$ for all $j \in [1, T]$.

1.2 Then it selects $\gamma \in RZ_{*p}$ and computes $w = g\gamma$. Subsequently, it selects $xi \in RZ_{*p}$ and computes $Ai = g\backslash(\gamma+xi)$ for all $i \in [1, N]$.

1.3 After that, it computes $Bij = hxi\, j$ for all i and j. The master public key mpk is $(g, \tilde{g}, h1, \ldots, hT, w)$. Each subscriber's secret key $[i]$ is (Ai, xi).

1.4 The revocation token at interval j of the subscriber with the secret key (Ai, xi) is $[i][j] = Bij$.

Step 2: VLR-GS. Sign (mpk, [i], j, M)

1. Select random number $\alpha, \beta, \delta \in RZ_{*p}$.
2. Compute $T1 = Ai \tilde{} g\alpha$, $T2 = g\tilde{\alpha}\, g\beta$, $T3 = e(gxi, hj)\, \delta$, and $T4 = g\delta$.
3. Compute $V = SPK\{(\alpha, \beta, \delta, xi, Ai): T1 = Ai \tilde{} g\alpha \wedge T2 = g\tilde{\alpha}\, g\beta \wedge T3 = e(gxi, hj)\, \delta \wedge T4 = g\delta \wedge e(Ai, wgxi) = e(g, g)\}(M)$.
4. Output the group signature $\sigma = (T1, T2, T3, T4, V)$.

Step 3: VLR-GS. Verify (mpk, j, RLj, σ, M)

1. Signature check. Check that σ is valid, by checking the $SPK\, V$.
2. Revocation check. Check that the signer is not revoked at interval j, by checking $T3 \neq e(T4, Bij)$ for all $Bij \in RLj$.

Step 4: Stop

3.3. Mobility Prediction Algorithm

We present another Module for reliable communications in SRRMP protocol called MPA. To improve the reliability of routing protocol along with security, we worked on mobility prediction based algorithm. We estimate the mobility-based path selection and select the more stable path. The proposed approach explained below.

Algorithm: Mobility based path estimation algorithm

- Step 1: When node i receive or overhears a packet P, IF the node i is the final destination address, consume the packet. GOTO END;
- Step 2: (Assume P belongs to <SAk,DAk> flow.) Compare <SAk,DAk> to all the valid entries in the hop comparison array;
- Step 3: IF there is no match with the entries, store <SAk,DAk,HCk,NAk> in the hop comparison array;
- Step 4: IF the packet is destined to i as the next-hop node, process the packet for forwarding further.
- Step 5: (Assume that it matched with an entry <SAk,DAk,HCj,NAj>) IF (HCk − HCj > 2), a short-cut is found, node i does the following:
- Step 5.1: Send a message to NAj to update the routing table such that the next-hop address for destination node DAk is modified to the address of node i;
- Step 5.2: Modify its routing table by making the next-hop address for destination DAk as NAk;
- Step 5.3: Modify its hop comparison array, delete the entry corresponding to <SAk,DAk>;
- Step 6: Return the efficient path.
- Step 7: Stop.

Mobility based Path Estimation Method: This is concerned with optimizing and healing paths to reduce the number of hops and hence improving the routing performance.

In our experiment showing the summary of detailed simulation parameters and its values of simulation configuration for varying mobility speed (5 m/s to 25m/s) with simulation time is 25s and transmission packet rate 10 m/s for 50 nodes of traffic patterns CBR (constant bit rate), network size 1000x1000,

MAC protocol 208.11, and channel data rate 11 Mbps using security method APALLS/ARAN/EAA/SRRMP. By doing this, it can achieve both extended network lifetime and secure routes for data transmission.

VI. SIMULATION RESULTS

Below tables are showing the summary of detailed simulation parameters and its values.

Table 4.1: Simulation Configuration of Varying Attackers

Number of Nodes	50
Traffic Patterns	CBR (Constant Bit Rate)
Network Size (X * Y)	1000 x 1000
Simulation Time	25s
Transmission Packet Rate	10 m/s
Pause Time	1.0s
Routing Protocol	APALLS/ARAN/EAA/SRRMP
MAC Protocol	802.11
Channel Data Rate	11 Mbps
Mobility Speed	5 m/s
Number of Attackers	1, 3, 5, 7 and 9
Number of Pairs	5

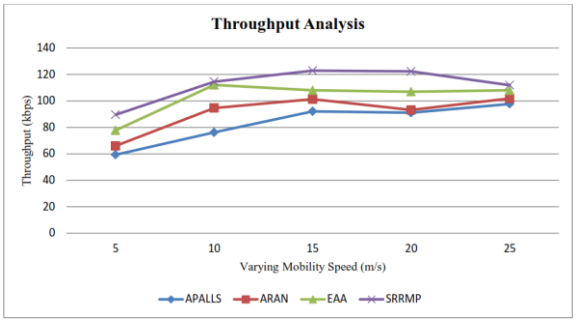

Figure 4.1: Average Throughput Analysis

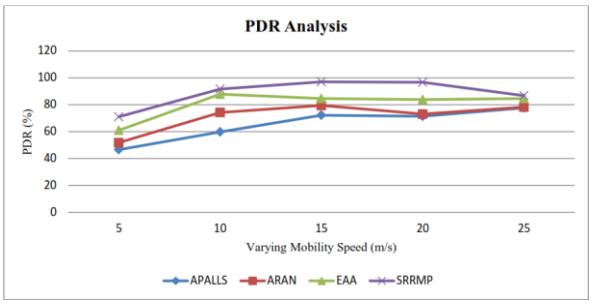

Figure 4.2: Packet Delivery Ratio Analysis

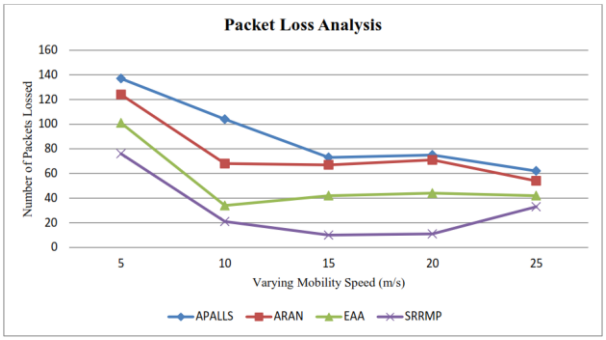

Figure 4.3: Packet Loss Ratio Analysis

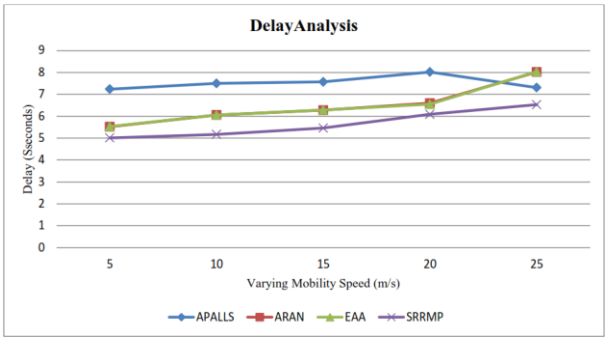

Figure 4.4: Delay Analysis

Figures 4.1 & 4.5 are showing that performance of throughput in case of proposed HEAA routing protocol is better as compared other methods for wireless network security. HEAA claiming that it can efficiently handle and mitigating the different malicious nodes attacks and preventing them from performing any kind of damage to wireless network security. The throughput performance is approximately improved by 25 % as compared to all previous methods.

Figures 4.2 & 4.6 are showing the success rate of data delivery to intended recipients. Most of the times it may possible that data may not deliver to the intended destination due to attackers. HEAA is solving this problem and producing better PDR performance.

Figures 4.3 & 4.7 are showing packet loss performance. HEAA is a combination of privacy preservation and secure communication algorithms; it provides two-day security to prevent any kind of data loss. The packet loss is very less for the proposed method. The performance of packet loss is minimized by 15 % approximately.

Figures 4.4 & 4.8 are showing the end to end delay performance. The earlier method is having a limitation of poor delay performance which is overcome by HEAA significantly. The delay is reduced by 20 % approximately as compared to EAA method.

Figures from 4.5 to 4.8 are showing below which according to a varying number of malicious nodes in the network.

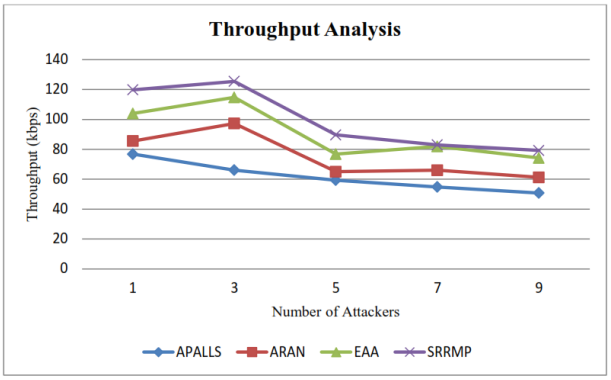

Figure 4.5: Performance Analysis of Throughput with Varying Number of Attackers

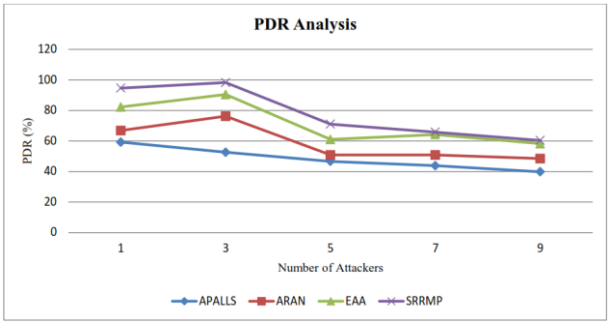

Figure 4.6: Performance Analysis of Packet Delivery Ratio with Varying Number of Attackers

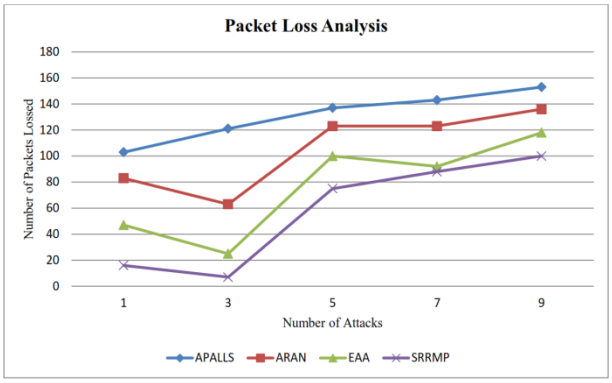

Figure 4.7: Performance Analysis of Packet Loss Ratio with Varying Number of Attackers

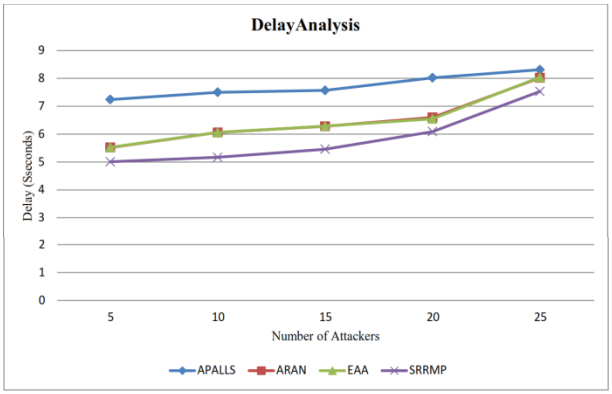

Figure 4.8: Performance Analysis of Delay with Varying Number of Attackers

V. CONCLUSION AND FUTURE WORK

Reliable routing in mobile ad hoc network is a challenging problem due to the dynamic and mobile nature of the network. It is demonstrated audits on the mobility prediction routing algorithms for mobile ad hoc networks. This greater mobility of nodes in MANETs points to the routing overhead in the route discovery. In this study, an attempt has been made to consider multiple routing metrics such as distance, cost, delay, load, and reliability in order to provide efficient, scalable, reliable and robust routing solutions. The commonly used classical routing protocols, in this research, use an objective vector that yields quality of service, reliability and efficient security in MANET routing. We presented an extensive literature survey study on different privacy preservation and authentication methods. Additionally, we presented related methods for secure MANET communication in this research. The goal was to present secure and reliable using mobility prediction routing protocol for MANET which is based on two methodologies such as efficient security algorithm and Mobility based Path Estimation Method. APALLS, ARAN and EAA as also our core Module for evaluation purpose, as previously these privacy-preserving method were not evaluated under real-time network scenarios such as MANET networks. The proposed routing protocol is called SRRMP which designed and simulated using NS3 and compared against three existing methods. The network scenario considered for performance evaluation is varying mobility speed under the presence of malicious user attacks. SRRMP is showing the throughput improvement by 30 % as compared to the EAA method. The packet loss performance is improved 10 %-15 % approximately as compared to EAA method. For future work, we suggest working scalability evaluations in terms of speed and network sizes.

REFERENCES

1. Adarbah, H.Y., Linfoot, S., Arafeh, B. & Duffy, A. (2012). 'Impact of the noise level on the route discovery mechanism in noisy MANETs', Proceedings of the first IEEE Global Conference on Consumer Electronics, pp. 699–703.

2. Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (n.d.) (2002).. A secure routing protocol for ad hoc networks. 10th IEEE International Conference on Network Protocols. Proceedings. DOI:10.1109/icnp.2002.1181388.

3. Mohemmed, A.W. & Sahoo, N.C. (2007). 'Efficient Computation of Shortest Paths in Networks Using Particle Swarm Optimization and Noising Met heuristics', Discrete

Dynamics in Nature and Society, vol., pp. 1–25.

4. Haigh, K.Z. (2006). 'Automatic Learning-based MANET Cross-Layer Parameter Configuration', 26th IEEE International Conference on Distributed Computing Systems Workshops ICDCS, pp. 1-7

5. Sivakumar Kulasekaran and Mahalingam Ramkumar (2011). "APALLS: A Secure MANET Routing Protocol" Mississippi State University USA, January 2011.

6. Khalid Zahedi & Abdul Samad Ismail (2011). 'Route Maintenance Approach for Link Breakage Prediction in Mobile Ad Hoc Networks', International Journal of Advanced Computer Science and Applications ((IJACSA), vol. 2, no. 10, pp. 23-30.

7. Han, Q., Gong, L., Wu, W. & Bai, Y. (2011). Link availability prediction-based reliable routing for mobile ad hoc networks. IET Communications, 5(16), pp. 2291–2300. DOI:10.1049/iet-com.2010.0946.

8. Ruchita, G., Divyanshu & Manoj, M. (2011). 'Quality of Service Provisioning in MANET using a Cross Layer Approach for Routing', International Journal of Computer Networks & Communications, vol. 3, no. 3, pp. 147-154.

9. Dillingham, R.F. (2007). 'Communicating on the Move: Mobile Ad-Hoc Networks', CROSSTALK the Journal of Defence Software Engineering, no. July, pp. 22–23.

10. Zhang, H. & Dong, Y. (2006). 'Mobility Prediction Model Based Link Stability Metric for Wireless Ad Hoc Networks', International Con

Corresponding Author

Satav Sandip Dattatraya*

PhD Student, Maharishi University of Information Technology, Lucknow