Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CROSS LAYER ENHANCED SECURE ROUTING SCHEME FOR AUTHENTICATION IN MOBILE AD HOC NETWORKS

C.SIVAMANI[1] and Dr.P. VISALAKSHI[2]

[1]Assistant Professor, Department of ECE, Angel College of Engineering &Technology.
Email: sivamanic123@yahoo.com
[2]Associate Professor, Department of ECE, PSG College of Technology
Email: visapsg@gmail.com

ABSTRACT

In recent years, mobile ad hoc networks provide new challenges and goals in fault tolerant computing area. Mobile nodes are communicated without any access point. In previous research works, fault tolerance has been achieved with or without the knowledge of checkpoint scheme. Due to high mobility of nodes in MANETs, there is always possibility of attacks among the agents which would result in performance degradation of the networks and damages the whole network connectivity. In this paper, a Cross Layer enhanced Secure Routing Scheme (CLSRS) is introduced for achieving fault tolerance level and authentication rate. Cross layer is deployed to improve the network lifetime and network performance. Cluster heads are chosen using trust threshold value based on signal strength and remaining energy level. Finally, digital signature generation and verification procedure is also proposed to authenticate packet as well as mobile agents. This scheme is integrated with diskless checkpoint protocol to achieve high fault tolerance rate. By using extensive simulation results, the proposed protocol CLSRS is observed to attain better performance when compared with approaches like Hybrid Cluster enhanced Stable Link Routing (HCSLR) and Cluster-based Certificate Revocation with Vindication Capability (CCRVC).

Keywords: *Cross Layer, Diskless Checkpoint, Cluster Head Election, Digital Signature Generation And Verification, Fault Tolerant Rate, Authentication Rate.*

1. INTRODUCTION

The Mobile Ad hoc networks contain several mobile nodes which are used to communicate among themselves without any fixed infrastructure. It is frequently used in special situations such as in emergency condition namely manmade disasters, rescue activities, battle fields or seminar halls particularly in areas where there is no fixed infrastructure or such infrastructure has been destroyed [1]. A node may either function as an end node or as a router forwarding data packets between source and destination nodes. Due to dynamic nature of ad hoc networks, packet integrity may get exploited and it will lead to network instable. In order to overcome these issues, effective routing mechanism is introduced to maintain acceptable service quality during communication between nodes.

A mobile ad hoc network is a self-governing system of mobile hosts connected by wireless links. There is no stationary communications such as base station. If two hosts are not in radio range, communication between them may pass via one or additional intermediate hosts that is twice as routers [2]. The hosts are open to move around randomly, therefore varying dynamically the network structure. Accordingly routing protocols must be adaptive and capable to maintain routes despite the changing network connectivity. Such networks are very useful in military and other considered applications such as emergency rescue or exploration mission, where cellular infrastructure is engaged or untrustworthy. Commercial applications are also possible home-area wireless networking, networking intelligent devices or sensors, communication between mobile robots, etc., where there is a necessity for ubiquitous communication services without the use of a fixed infrastructure. As in [3], in recent times with the development of chip technology, handheld devices have sooner processing power and consume less energy. There are momentous differences between wireless and wired network. Wired networks have comparatively high bandwidth and topology which changes infrequently.

The following issues arise from the malicious activities in secure routing:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- **Broadcast errors**: The transmitted packets are getting stained and therefore received in error owing to the unreliability of the wireless medium and the fickleness of the environment.

- **Mobile Node failures**: Due to different types of risky conditions in the environment, nodes may fail at any cost. It may possibly drop out of the network either willingly or when their energy supply is at a low level.

- **Path failures**: Node failures in addition to varying environmental conditions may reason to break the paths between nodes.

- **Ruptures of path**: Due to high dynamic topology rate, network and path failures occur rapidly. Packets are forwarded through stale routes may either be dropped or be delayed based on the transport protocol.

- **Congested nodes**: Certain nodes may turn into congested owed to the topology of the network and the nature of the routing protocol. This will go ahead to either larger delays or packet loss.

The multipath routing is proposed as an alternative to single shortest path routing to distribute load and improve congestion in the network. In multipath routing, traffic bound to a destination is divided across multiple paths to that destination. Accordingly, multipath routing uses multiple "good" paths in preference to a single "best" path for routing. Multipath routing aims to set up multiple paths between source-destination pairs and therefore need more hosts to be answerable for the routing tasks.

1.1. Contribution of the work

- Cluster heads are chosen based on signal strength and energy level.

- Cross layer is deployed to improve the link quality.

- Digital signature generation and verification procedure is used to authenticate packet as well as mobile agents.

- Proposed scheme is integrated with diskless checkpoint protocol to achieve high fault tolerance rate.

.

2. LITERATURE SURVEY

In Goswami and Anshu Chaturvedi [4] proposed effective cluster-head Selection that selects a Cluster-head node who is trustworthy enough. Thus the route discovery and maintenance system are secured. Moreover the scheme holds the disconnections in ad hoc network due to the effects of topology variation. The algorithm put forward a cross-layer approach that incorporate Cluster head discovery and selection process with ad hoc network routing mechanism also the lower layer driver's included in the system. This scheme allows clients to change to improved Cluster-head nodes changes the network structure. Therefore, the proposed scheme provides better performance to network.

Mamatha [5] presented cross layer architecture. The proposed scheme with a new routing mechanism is called as protocol less approach, encryption technique and an acknowledgement approach, the structural design make sure that it safe guards the data packet forwarding to maximum extent. Thus this mechanism covers the security aspects of three layers as presentation layer, transport layer and network layer. In any of these systems, one cannot look forward to the three components i.e. providing security, detection and correction and recovery for transmission. Here it provides authentication to control and data packets.

In [6] a cross layered model for congestion detection and control mechanism that consist of energy efficient congestion detection, Zone level Congestion Evaluation Algorithm (ZCEA) and Zone level Egress Regularization Algorithm (ZERA), which is hierarchical cross layer based congestion detection and control model. By analyzing the results, the proposed approach attains better resource utilization, energy efficiency in congestion detection and congestion control when compared with other existing algorithms.

Rakesh Shrestha et.al [7] proposed a novel cross layer intrusion detection approach to discover the malicious nodes and different types of DoS attacks by using the information presented across different layers of protocol stack to improve the precision of detection. The approach uses

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cooperative anomaly intrusion detection with data mining approach to improve the system. It is implemented with fixed width clustering algorithm for efficient detection of the anomalies in the MANET traffic.

Ravneet Kaur [8] proposed the Cross layer based miss detection ratio under variable rate for intrusion detection in WLAN. Here, the decision is based on the combination on weight value of two or more layer. So the result is not based on single layer, it will reduce false positive rate. Two different layers, physical and MAC have been used in this research and the results have been evaluated with existing approaches.

Salman Khan [9] proposed Thread Level Speculation (TLS) which relieve the programmer and compiler from checking for thread dependences and in its place use the hardware to enforce them. Unluckily, TLS suffers from power in efficiency because data mispeculations cause threads to roll back to the start of the speculative task. Therefore intermediate check pointing of TLS threads has been presented. When an abuse does occur, it now has to roll back to a checkpoint before violating instruction and not to the start of the mission. However, earlier work excludes study of the micro-architectural details and implementation problems that are necessary for effective checkpointing.

Wei Liu et.al [10] proposed the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme to improve the reliability of the scheme, to make progress the warned nodes to be included in the certificate revocation process. As well as, the threshold-based mechanism was proposed to assess and vindicate warned nodes as legitimate nodes or not, before recovering them.

3. METHODOLOGY

The proposed cross layer enhanced checkpoint protocol is based on cluster head selection, optimized signature generation and verification of data during transmission and the design is carried out using the cross layer design.

3.1 Cross Layer design

In Fig.1, cross layer infrastructure is shown to illustrate the communication between the sender and receiver [11]. In sender part, packet dropping measurement is done and queue length is measured at the receiver part. Because of crossing network layer and transport layer, a reliable end to end transmission is successfully achieved. With this, cross layer structure will keep on watching the link quality. The performance of the channel is determined by MAC layer, the data transmission gets started. The mobile agent at the destination end observes the power levels of each received transmission from the receiver. When the source mobile agent receives this notification, then it immediately halts the transmission, the expected fade duration is determined and schedules future transmissions accordingly. The Network Allocation Vector (NAV) at the neighbors is also updated when they overhear a CTS or ACK whose flag bit is marked. The simulation results using object oriented discrete even simulator that indicates the cross-layer implementation performs better than the layer implementation in terms of received signal strength throughput, fraction of packets dropped, throughput, delivery ratio and congestion ratio.

In the proposed cross layer framework, cluster head monitor the congestion status, packet dropping measurements through the network layer. End to end transmissions are performed in transport layer. In any packet suffers from delay or duplication, an REPORT_ACK packet will be reached to cluster head. So the cluster head will choose any alternative secure routes are available or not. Signature generation and verification are performed in network layer itself. As the status of the packet are monitored only in cross layer.

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

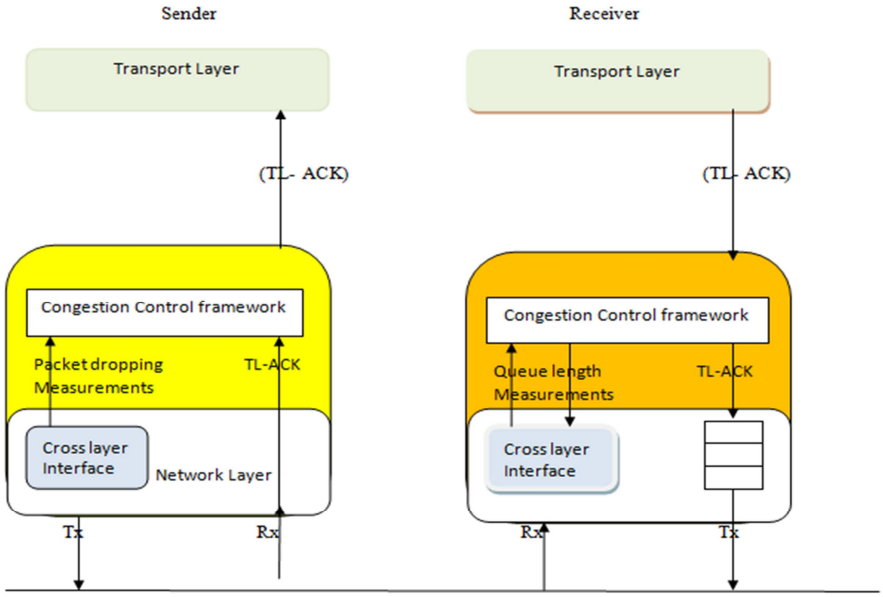

Fig.1. Cross Layer Infrastructure

3.2 Cluster head Selection Procedure

The selection of Cluster heads are considered in computing systems of n nodes such that every node in this network is within distance h hops of a CH, for a given threshold value [12]. In the proposed model, the Cluster lifetime denotes the time from the point a node is elected as Cluster head until the point a node changes its status to normal node and depends on more remaining battery lifetime. The Cluster lifetime is dependent on mobility issues, the Cluster lifetime in Mobile computing systems which depends on link stability, link quality. In this procedure, a cluster message is sent every 5 seconds. Thus, a neighbor agent is kept in the neighbor table for 5 *COUNTR seconds and discarded if there is no further Clustering message received. Initially, the cluster head table (CHT) for all nodes has been considered as null or 1. Owing to the dynamic changes in the topology of network, the Cluster formation is simplified from time to time. When a node forwards a packet, it loses some amount of energy whose amount is based on the factors such as the nature of packets, their size, right to use frequency, and the distance between the nodes [13].

Therefore it is considered to be an individual energy power in assuming the path, i.e., if there is a path with a node having very low energy level and after that the existing power function does not choose that path, irrespective of whether or not that path is time efficient [14].

// Cluster formation procedure
Input: Set of mobile agents
Output: Set of clusters
Begin Cluster =L /* represent cluster number L */
Repeat
Select a agents b_k which is 1 hop distance apart from
other participating nodes with a small length d_l randomly
Do N = b_k ; d= d_l
Draw a circle with b_k as center and d as radius
Compute new radius (d_l) = d + |b_k-b_q|
while $b_k \neq b_q$
Cluster-L is formed with cooperating nodes lying within
the circle; End

// Cluster head selection procedure
$TA_{cur} \leftarrow 0$
$T_{RSSI} \leftarrow 0$
$TA_{prev} \leftarrow 0$
$Time_{prev} \leftarrow 0$
now() $\leftarrow 0$
Time – OUT loop $\leftarrow$ 5*COUNTR
Interaction history (IH) ≥ 0
while Timeprev $\leq$ now() or
Threshold (TAprev) ≤ 1 = true do
TA_{prev} remains as Cluster head
end while
if threshold (TA_{prev}) = threshold (TA_{cur}) and
CHT (TA_{prev}) = CHT (TA_{cur}) then
both TA_{prev} and TA_{cur} remain as Cluster heads

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

else
select new Cluster head(s)
end

3.3 Optimized signature generation and verification Scheme (OSVS)

The Optimized signature scheme is a randomized signature mechanism which produces digital signatures by means of appendix on binary messages of arbitrary length, and needs a hash function h: {0, 1} → Z_p where p is a large prime number. The digital signature scheme is a variant of the Optimized signature mechanism [15]. Each entity creates a public key and equivalent private key. Each entity chooses a finite group G; generator of G; public and private keys.

Each entity A should do the following:

1. Generate a large random prime p and a generator α of the multiplicative group Z^*_p.
2. Select a suitable cyclic group G of order n, with generator α. (Consider G is written multiplicatively.)
3. Select a random integer a, $1 \le a \le p - 2$, calculate $y = \alpha^a \bmod p$.
4. Select a random secret integer a, $1 \le a \le n-1$. Calculate the group element $y = \alpha^a$.
5. A's public key is (p,α, y), jointly with a explanation of how to multiply elements in G.

Entity signs a binary message m of arbitrary length. Several entity B can confirm this signature by means of A's public key.

1. Signature generation. Entity A should do the following:
   a. Select a random secret integer k, $1 \le k \le p - 2$, with gcd (k, p − 1) = 1.
   b. Compute $r = \alpha^k \bmod p$
   c. Compute $k^{-1} \bmod (p - 1)$
   d. Compute $s = k^{-1}\{h(m) - a^r\} \bmod (p - 1)$.
   e. A's signature for m is the pair (r, s).
   i. Compute the group element $t = \alpha q$.
   ii. Compute $q^{-1} \bmod n$.
   iii. Compute h(m) and h(r).
   iv. A's signature for m is the pair (r, s).
2. Verification. To verify A's signature (r, s) on m, B should do the following:
   a. Obtain A's authentic public key (p, α, y).
   b. Verify that $1 \le r \le p - 1$; if not, then reject the signature.
   c. Compute $v_1 = y \bmod p$.
   d. Compute h(m) and $v_2 = \alpha\, h(m) \bmod p$.
   e. Compute $g_1 = yh(r) \cdot rs$.
   f. Compute $g_2 = \alpha h(m)$.
   g. Accept the signature if and only if $v_1 = v_2$.
   h. Accept the signature if and only if $g_1 = g_2$.

Proof:

If the signature was generated by A, then $s \equiv k^{-1}\{h(m) - a_r\} \pmod{p-1}$. Multiplying both sides by k gives $ks \equiv h(m) - ar \pmod{p-1}$, and reschedule capitulate $h(m) \equiv ar + ks \pmod{p-1}$. This implies $\alpha h(m) \equiv \alpha^a r + ks \equiv (\alpha^a) r\, s \pmod p$. Therefore, $v_1 = v_2$, as required.

Key generation: A selects the prime p = 2357 and a generator α = 2 of 2357. A chooses the private key a = 1751 and measures $y = \alpha^a \bmod p$ = 21751 mod 2357 = 1185. A's public key is (p = 2357, α = 2, y = 1185).

Signature generation. For simplicity, messages will be integers from Zp and h(m) = m (i.e., for this example only, take h to be the identity function). To sign the message m = 1463, A selects a random integer k = 1529, computes $r = \alpha k \bmod p$ = 21529 mod 2357 = 1490, and $k^{-1} \bmod (p - 1)$ = 245. Finally, A computes $s = 245\{1463 - 1751(1490)\} \bmod 2356 = 1777$. A's signature for m = 1463 is the pair (r = 1490, s = 1777).

Signature *verification*. B computes v_1 = 11851490 · 14901777 mod 2357 = 1072, h(m) = 1463, and v_2 = 21463 mod 2357 = 1072. B accepts the signature since $v_1 = v_2$.

An opposition may attempt to form A's signature on m by selecting a random integer k and calculate $r = \alpha^k \bmod p$. The opposition be required to determine $s = k^{-1}\{h(m) - a^r\} \bmod (p - 1)$. If the discrete logarithm issue is computationally infeasible, the opposition can do no better than to choose an s at random; the success probability is only 1 p, which is omitted for large p.

The flow diagram of the proposed scheme is show in figure 2. In this scenario, each cluster heads communicate through the cluster members while keeping diskless checkpoint protocol. The signature generation and verification scheme are also deployed in each and every packet from source to destination. This makes data with higher data integrity and to identify the authenticated cluster head or source mobile agent.

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

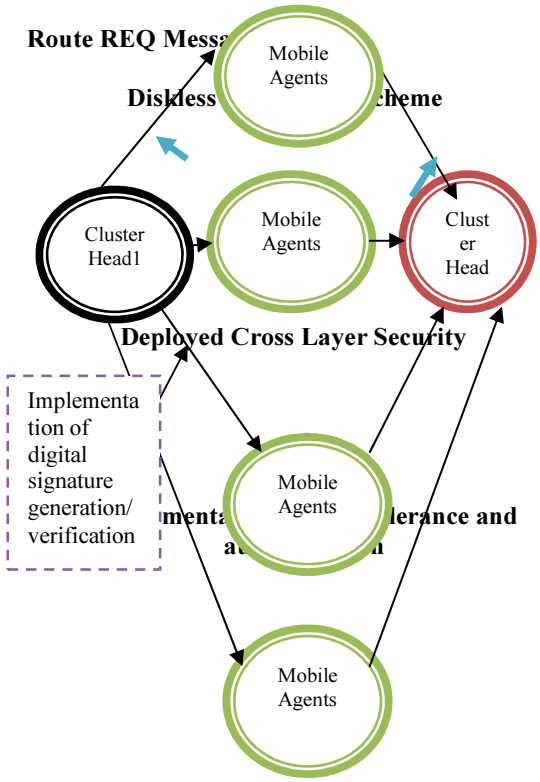

Fig.2. Flow chart of Proposed Scheme

3.4 Proposed packet format

Source ID	Destination ID	Hop Count	Data Integrity	Fault tolerant rate	FCS

Fig 3. Proposed Packet format

In figure 3, the proposed packet format is shown. Here the source and destination node ID carries 2 bytes. The third field hop count predicts the number of n does connected to the particular node in the cluster which occupies 1 byte. The data integrity persuades whether the transmission of packets is travelled with high integrity from the source node to the destination node. Fault tolerant rate is verified through the route maintenance phase occupies 4 bytes. The last filed FCS i.e. Frame Check Sequence which is for error correction and detection in the packet while transmission.

4. PERFORMANCE ANALYSIS

The proposed cross layer enhanced checkpoint protocol is integrated with the DSR protocol. The Network Simulator (NS 2.34) is employed to simulate the proposed algorithm. In this simulation, 300 mobile nodes are in motion in a 1500 meter x 1500 meter square region for 120 seconds simulation time. All the agents have same transmission range of 300 meters. The simulated traffic is Constant Bit Rate (CBR) and Poisson traffic. Simulation settings and parameters are summarized in table 1.

Table1. Simulation settings and parameters

No. of mobile nodes	101
Area Size	1500 X 1500
Radio Range	300m
Simulation Time	120 sec
Traffic Source	CBR and Poisson
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	Dynamic Source Routing
Pause time	5 msec
Packet Queuing	Drop Tail

A. Performance Metrics

The proposed approach evaluates the performance according to the following metrics.

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Throughput: It is defined as the number of packet received at a particular point of time.

Authentication rate: It is defined as how much number of packets are identified correctly with respect to faulty packets.

Fault tolerant rate: It is the ratio of number of packets with corrupted through the specified path. This ratio should be kept maximum.

The simulation results are presented in the next part. We compare our CLSRS with our previous scheme HCSLR and CCRVC protocol [15] in presence of congestion environment. Figure 4 shows that traffic creation among the nodes. To

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

identify the packet loss, the constant bit rate traffic is implemented. The delay is produced in packet from source agent to destination agent via neighbor mobile agents. Source may choose the different paths to achieve the high packet delivery fraction.

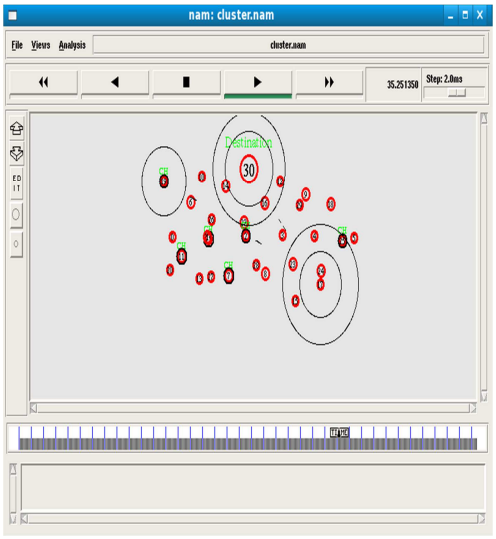

Fig. 4. Topology and Traffic creation

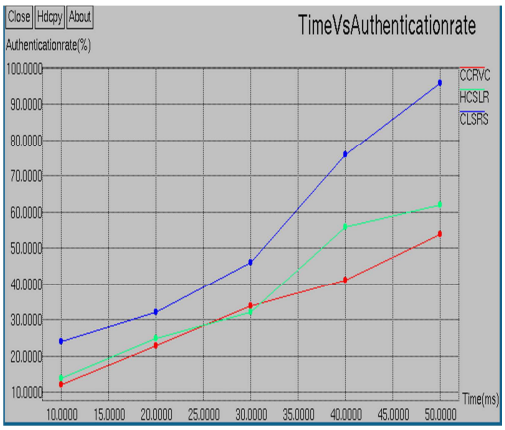

Fig. 5. Time Vs Authentication Rate

Figure 5 shows the results of packet authentication rate for varying the time from 10 to 50 msecs. From the results, we can see that CLSRS scheme has high authentication rate than the CCRVC and HCSLR schemes because of secure checkpoint protocol. It is because of optimized signature generation and verification. Authentication rate implies that how many packets and nodes are authenticated to improve the fault tolerant level. This will lead to more security.

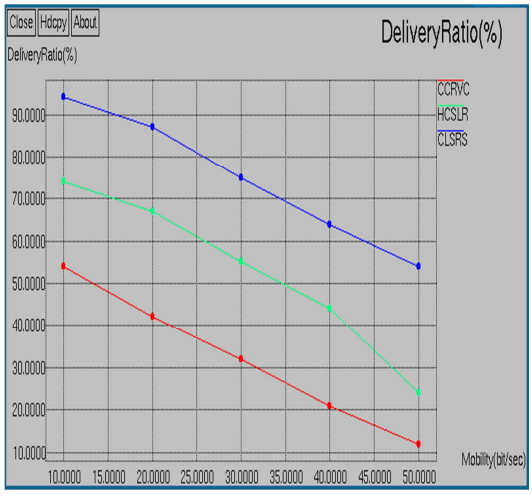

Fig. 6. Mobility Vs delivery ratio

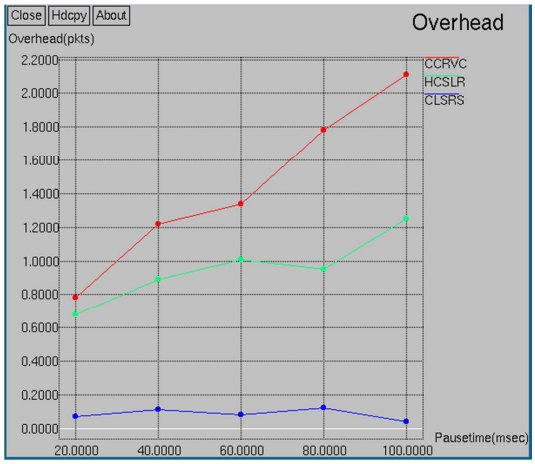

Fig. 7. Pause time Vs Overhead

Fig.6 shows the packet delivery ratio with increasing mobility. As mobility increases, the wireless link disconnectivity also gets increasing. This will lead to network partition. So the packet delivery ratio may able to get decreases. In previous schemes CCRVC, it was only concentrated on cross layer routing. But in CLSRS, it was exploited that encryption and decryption procedure. Simulation time increases which increases node mobility but less packet drops occurs in CLSRS. So our proposed scheme achieves 94- 54% deviation over HCSLR and CCRVC. The proposed scheme CLSRS deliver more authenticated packets compared to existing schemes.

Fig. 7, presents the comparison of overhead and pause time. When pause time increases, communication will be suppressed between the source and destination. It is clearly shown that the overhead of CLSRS achieved 0.07-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

0.04 packets ratio than the HCSLR and CCRVC protocol. The probability of sending control packets are getting decreased because of integrating secure authentication scheme.

Figure 8 shows the results of Speed Vs Network Lifetime. From the results, we can see that CLSRS scheme has higher Network Lifetime (620.56-1600.33) milliseconds than the CCRVC protocol and HCSLR while varying the speed of mobile agents from 10 to 200. The unwanted node communication is reduced which increases whole network lifetime in the proposed scheme.

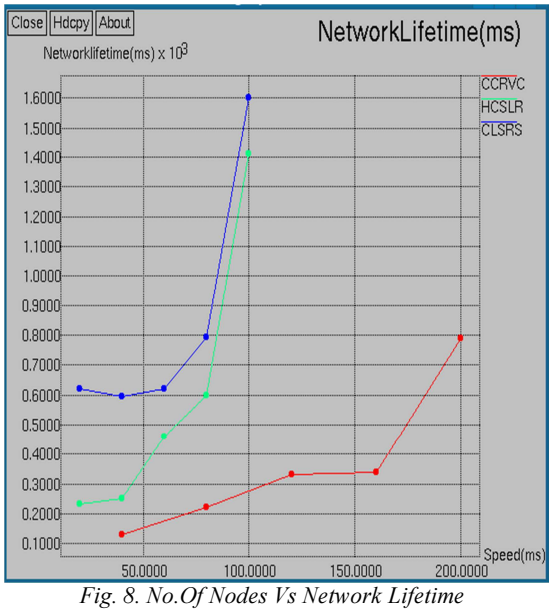

Fig. 8. No.Of Nodes Vs Network Lifetime

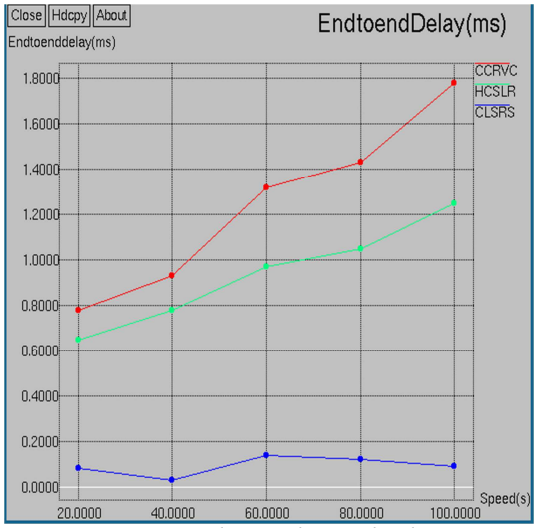

Fig. 9. Speed Vs End To End Delay

Figure 9, presents the comparison of End to end delay while varying the Speed from 20 to 100 secs. It is clearly shown that the delay of CLSRS achieves 0.08-0.09 seconds than the HCSLR and CCRVC protocol. Delay of proposed scheme is decreased because of keeping genuine packets in the path and making pause time between the packets low.

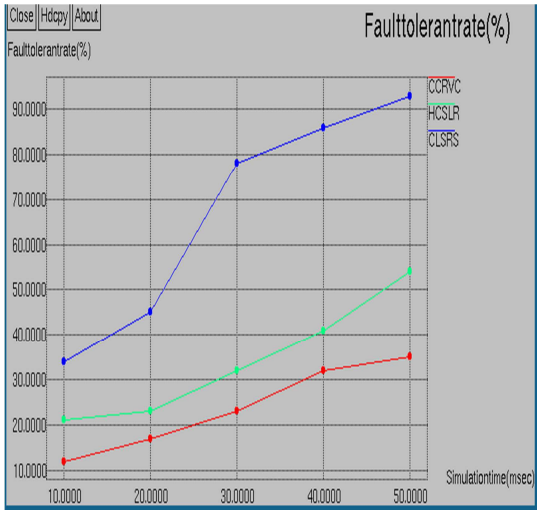

Fig. 10. Simulation Time Vs Fault Tolerant Rate

Figure 10, presents the comparison of fault tolerant rate while varying the Simulation time from 10 to 100ms. It is clearly shown that the fault tolerant rate of CLSRS achieves 34-93 ratio than the HCSLR and CCRVC protocol. When it is combined both fault tolerant routing and network authentication, fault tolerant rate is automatically increased. Our proposed scheme CLSRS achieves 96% rate than previous schemes.

5. CONCLUSION AND FUTURE WORKS

Due to high mobility of mobile agents, performance of network gets degraded. To avoid and handle fault tolerant level, several techniques with or without checkpoint protocol is proposed. But there is a lack of data authentication and fault tolerant rate in these studies. In the presence of the attacks, the data is collapsed or damaged. In this paper, a Cross Layer enhanced Secure Routing Scheme is proposed for authentication and fault tolerant which attains the integrity and confidentiality among mobile agents. By using the extensive simulation results, the proposed scheme CLSRS achieves the better authentication rate, packet delivery ratio, fault tolerant rate, network lifetime low delay and overhead than the existing schemes like CCRVC and HCSLR while varying the mobility, time, simulation time, pause time and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

speed. In future, plan to implement secure secret sharing scheme to provide high security and data integrity.

REFRENCES:

[1] Joselin Retna Kumar G and Shaji KS, "Enhanced Channel Estimation Technique for MIMO-OFDM Based Communications Using Neuro Fuzzy Approach", 2012 *International Conference on Conference on Signal Processing Systems* (ICSPS 2012),

[2] Shakkeera, "Optimal path selection technique for flooding in link state routing protocol using forwarding mechanisms in MANET," in *International Conference on Communication and Computational Intelligence, (INCOCCI2010),* Erode, India, pp. 318-323, 2011.

[3] Asis Nasipuri and Robert Castañeda, "Performance of Multipath Routing for On-Demand Protocols in Mobile Ad Hoc Networks", *Mobile Networks and Applications* 6, 339–349, 2001.

[4] An Huiyao, Lu Xicheng, and Peng Wei , " A Cluster-Based Multipath Routing for MANET", Supported by *National Momentous Foundation Research task*, 2003, pp.405-313.

[5] D. N. Goswami and Anshu Chaturvedi, "Cross Layer Integrated Approach for Secured Cluster Selection in Ad Hoc Networks", *International Journal of Computer and Communication Engineering*, Vol. 1, No. 3, September 2012, pp.187-190.

[6] G. S. Mamatha," A Defensive Mechanism Cross Layer Architecture for MANETs to Identify and Correct Misbehaviour in Routing", *International Journal of Network Security & Its Applications (IJNSA),* Vol.4, No.1, January 2012, pp.117-126.

[7] Xiaoxia Huang& Yuguang Fang, "Multiconstrained QoS multipath routing in wireless sensor networks", *Wireless Networks, Springer*, Vol.14, 2008, pp.465–478.

[8] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han, " A Novel Cross Layer Intrusion Detection System in MANET", *IEEE International Conference on Advanced Information Networking and Applications*, 2010, pp.647-654.

[9] Ravneet Kaur, "Cross layer based miss detection ratio under variable rate for intrusion detection in WLAN", *International Journal of Computer Engineering Research,* Vol. 2(5), November 2011, pp. 75-81.

[10] Salman Khan, Nikolas Ioannou, Polychronis Xekalakis &Marcelo Cintra, "Increasing the Energy Efficiency of TLS Systems Using Intermediate Checkpointing", *IEEE Conferences*, 2011, pp.1-10.

[11] Wei Liu, Student Member, IEEE, Hiroki Nishiyama, Member, IEEE, Nirwan Ansari, Fellow, IEEE, Jie Yang, and Nei Kato, Senior Member, IEEE, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol.24, No.2, 2013, pp.239-249.

[12] Jens Mittag, Stylianos Papanastasiou, Hannes Hartenstein, Erik G. Strom, "Enabling Accurate Cross-Layer PHY/MAC/NET Simulation Studies of Vehicular Communication Networks", Proceedings of The IEEE - PIEEE , vol. 99, no. 7, pp. 1311-1326, 2011

[13] Abderrezak Rachedi, Abderrahim Benslimane, "Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks" *International Conference on Systems and Networks Communications* - ICSNC , 2006

[14] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[15] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," *ACM Trans. Computer Systems*, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[16] Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks," *IEEE Trans. Dependable and Secure Computing*, vol. 2, no. 3, pp. 233-247, July 2005.