CDMA BASED SECURE CROSS LAYER FRAMEWORK FOR AUTHENTICATION AND SCHEDULING IN MANET

[1] B.BERIL DANIEL ROSARIO, [2]Dr.A.RAJARAM
[2] Research Scholar, Karpagam University, Coimbatore, India
[1]Associate Professor, Department of Electronics and Communication Engineering,
Karpagam University, Coimbatore, India.
E-mail: [1]berilkuphd@gmail.com, [2]gct143@gmail.com,

ABSTRACT

In MANET, mobile nodes are connected without any centralized administration. Due to that, a mobile node is easily affected by means of several attacks. Due to these attacks, network is totally partitioned and more packet congestion occurs. Because of improper scheduling, congestion level of network will get increase unlimitedly. To provide an authenticity of data packets and avoiding more congestion, there is a need of secure and scheduling mechanism in networks. In this research paper, we developed a CDMA based Secure Cross layer framework for authentication and scheduling. Here the cross layer is introduced to improve the quality and lifetime of nodes as well as links. The scheduling procedure is proposed to reach the packets in a time slot manner. In authentication phase, we proposed the modified concept of RSA scheme. Here the asymmetric key is chosen. Both encryption and decryption phases are used to validate the cipher text and manipulate the plaintext according the given message. By using extensive simulation, the proposed scheme achieves better throughput, packet delivery ratio, low end to end delay and overhead than the existing schemes.

Keywords: *MANET, Security, Cross Layer, Scheduling Time Slot, Authentication, Delivery Ratio, Packet Loss, Congestion Status, Packet Integrity And End To End Delay.*

1. INTRODUCTION

A. *Mobile Ad Hoc Networks (MANET)*

A MANET consists of a dynamic collection of nodes with sometimes rapidly changing multihop topologies that are composed of relatively low-bandwidth wireless links. There is no assumption of an underlying fixed infrastructure. Nodes are free to move arbitrarily. Since each node has a limited transmission range, not all messages may reach all the intended hosts. To provide communication through the whole network, a source-to-destination path could pass through several intermediate neighbor nodes. Unlike typical wireline routing protocols, ad hoc routing protocols must address a diverse range of issues. The network topology can change randomly and rapidly, at unpredictable times. Since wireless links generally have lower capacity, congestion is typically the norm rather than the exception. The majority of nodes will rely on batteries, thus routing protocols must limit the amount of control information that is passed between nodes. The goal of MANETs is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes form the network routing infrastructure in an ad hoc fashion. The majority of applications for the MANET technology are in areas where rapid deployment and dynamic reconfiguration are necessary and the wireline network is not available. These include military battlefields, emergency search and rescue sites, classrooms, and conventions where participants share information dynamically using their mobile devices.

B. Need for Cross layer Design in MANET

The requirement of Cross Layer design in ad hoc networks is given below.

Adaptivity and Self-Organization:

Network protocols for MANETs must be adaptive to many factors to effectively support fair sharing of devices and resources and to hide the system dynamics to the upper layers. The system dynamics include a wide range of communication conditions a wireless node can experience inside a MANET, including changing topology, shared medium contention, varying traffic patterns and distributions. The adaptive behaviour can be implemented if the following requirements are met:

• context awareness, i.e. the knowledge of the parameters affecting the network state (channel condition, congestion, traffic demands, etc);

• protocol tuning, i.e. the possibility for each protocol to adjust his behaviour according to the current network state.

Energy Conservation:

It is a limiting factor in the successful deployment of MANETs, because nodes are expected to rely on portable, limited power sources. Moreover, energy conservation is extremely challenging in multi-hop environments, where the wireless nodes should also consume energy to route packets for other nodes and to guarantee the connectivity of the network. At the MAC layer, some techniques can be used to reduce the energy consumed during transmission and reception; additionally, a careful policy may turn off the wireless device when the node is idle. At the network layer, the route selection process should be performed by reducing the end-to end power needed to forward the packet. If the network layer may have access to energy information, battery-level metrics can be used in the routing process.

Security:

Because nodes in MANETs communicate each other via open and shared broadcast channel, they are more vulnerable to security attacks. Moreover, the support for multi-hop communication implies that the network has to rely on individual solutions from each mobile node, resulting vulnerable to infiltration, eavesdropping, interference, DoS attacks. Many research efforts have mostly concentrated on secure data forwarding: secure routing protocols face the attacks that intentionally disrupt the routing protocol execution, and guarantee the acquisition of correct topological information. On the other hand, data-link security solutions are implemented as parts of wireless standards (WEP/WPA for 802.11) to provide authentication and privacy issue on infrastructured single-hop wireless networks. However, the solutions proposed at MAC, routing and transport layer only cover a subset of all possible threats. A cross-layer design of MAC, routing and transport protocols allows to take into account the security issues in all the stages of protocol design.

2. RELATED WORK

Asmidar Abu Bakar et.al [1] developed the secure access architecture consists of trust management, access control policy and cryptology protocols. With the proposed architecture, a comprehensive access control model is constructed to support the access to data and information required during emergency rescue mission. Using the access control model, members will be verified using the cryptographic protocols such as encryption/decryption, hash function and digital signature. This will ensure that only authenticated member, belong to correct group get an access to the information requested. The used of tag which was created prior to network setup, enabled members to be authenticated hence create trust. Beside this, the access policy embedded in the tag also able to distinguish the role between members' of the group at the emergency rescue mission. This will eliminate wrongly data passing between members in the group, hence ensuring data security and privacy is preserved.

D. N. Goswami and Anshu Chaturvedi [2] explored an algorithm called effective cluster-head Selection which selects a Cluster-head node who is trustworthy enough. Thus the route discovery and maintenance system are secured. Moreover the scheme handles the disconnections in ad hoc network due to the effects of topology changes. The algorithm put forward an effective cross-layer approach that integrates Cluster head discovery and selection functionality with network ad hoc routing mechanisms and the lower layer drivers built-in the system. This scheme allows clients to switch to better Cluster-head nodes as network topology changes. Hence, provides better performance to network.

Djallel Eddine Boubiche et.al [3] proposed intrusion detection system where cross layer interaction is heavily exploited. The proposed approach is used to provide a single cross layer IDS to several layers of OSI model. The approach does not claim to be immune from all security attacks towards WSN security. The cross layer interaction is happening between the network, Mac and physical layers. Indeed they have addressed the problem of intrusion detection in a different way in which the concept of cross layer is widely used leading to the birth of a new type of IDS.

Rekha Patil et.al [4] proposed a cost based power aware cross layer design to AODV. The discovery mechanism in this algorithm uses Battery Capacity of a node as a routing metric. This approach is based on intermediate nodes calculating cost based on Battery capacity .The intermediate node judges its ability to forward the RREQ packets or drop it. That is it integrates the routing decision of network layer with battery capacity estimation of MAC layer. The low power nodes are identified and rejected in RREQ flooding phase itself and not after facing any RREP transmission failures.

Kazuya et.al [5] analyzed a routing protocol that uses multi-agents to reduce network congestion for a Mobile Ad hoc NETwork (MANET). MANET is a multi-hop wireless network in which the network components such as PC, PDA and mobile phones are mobile. The components can communicate with each other without going through a server. Two kinds of agents are engaged in routing. One is a Routing Agent that collects information about network congestion as well as link failure. The other is a Message Agent that uses this information to get to their destination nodes.

Xiaoxia Huang and Yuguang Fang [6] introduced QoS multipath routing to provide soft QoS to different packets as path information is not readily available in wireless networks. The multiple paths are utilized between the source and sink pairs for QoS provisioning. Unlike E2E QoS schemes, soft-QoS mapped into links on a path is provided based on local link state information. By the estimation and approximation of path quality, traditional NP-complete QoS problem can be transformed to a modest problem. The idea is to formulate the optimization problem as a probabilistic programming, then based on some approximation technique, we convert it into a deterministic linear programming, which is much easier and convenient to solve. More importantly, the resulting solution is also one to the original probabilistic programming.

Laurence et.al [7] proposed a cross-layer distributed power control and scheduling protocol for delay-constrained applications over mobile CDMA-based ad hoc wireless networks. Herein, it is proposed that novel scheme where power control is employed to combat delay occurring on multi-hop wireless ad hoc networks via cross-layer information exchange. Based on that, a distributed power control and scheduling protocol is proposed to control the incurred delay as well as the multiple access interference (MAI).

In this paper [8], it was implemented that authentication method using ESA (Enhanced Subscriber Authentication) algorithm. Authentication mechanism using ESA algorithm uses AKA (Authentication and Key Agreement) to enhance security strength and to provide mutual authentication between a base station and a mobile terminal. But in this paper, there was a lack of packet integrity and authentication in routing. But our paper achieves more integrity and high scheduling rate than the existing works.

In this paper [17], an unobservable routing protocol USOR was proposed based on group signature and ID-based cryptosystem for ad hoc networks. The design of USOR offers strong privacy protection—completes unlinkability and content unobservability—for ad hoc networks. The security analysis demonstrates that USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise.

The paper is organized as follows. The Section 1 describes with overview of MANET and Need for Cross layer Design. Section 2 deals with the Related Work. Section 3 is devoted for the implementation of proposed algorithm. Section 5 describes the performance analysis and the last section concludes the work.

3. IMPLEMENTATION OF PROPOSED ALGORITHM

Our proposed cross layer based security scheme is based on received signal strength, encryption and decryption of data during transmission, and the design is carried out using the multipath routing.

A. *Cross Layer framework*

In our proposed scheme, a cross-layer design is proposed while the MAC layer predicts the state of the channel whether it is good or bad. This calculation depends on Rayleigh fading channel model where using the previous signal strength requirements. Once the channel is good which is determined by MAC layer, the data transmission gets started. The prediction model for the Rayleigh fading channel is cooperated with a Markovian model for IEEE 802.11 standards MAC to analyze the performance of the proposed scheme. The main reason for predicting the Rayleigh fading channel is to improve performance of the network. The mobile node at the destination end observes the power levels of each received transmission from the receiver. When the source node 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 obtained indicate 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.

B. CDMA based Scheduling Procedure

Let us consider the CDMA based scheduling procedure to divide the transmitter receiver pairs into subset and this is done through energy optimisation problem as follows:

$$\min F(K,M) = M\sum_{i=1}^{N} K_i \qquad (1)$$

$$\frac{P_{kl}G_{kl}}{\frac{1}{L}\sum_{n=1,n\neq l}^{L} P_{kn}G_{kl} + \frac{1}{L}\sum_{q=1,q\neq k}^{L}\sum_{n=1}^{L} P_{qn}G_{nl} + \sigma^2} \geq \chi \qquad (2)$$

The solution of the above optimisation problem results in 2M + 1 equations with 2E + 1 unknowns, which we can solve for P and L.

$$\frac{-1}{\varphi^2}\sum_{e=1}^{E} P_e + \alpha\sum_{e=1}^{E}\lambda_e \sum_{d=1,d\neq e}^{E} P_d G_{de} = 0 \qquad (3)$$

The solution provides the optimum spreading gain and the transmitter powers for all transmitters. Here, it is worth to be mansion that transmission power control is automatically taken care of by the optimisation problem as we optimise total network energy.

The algorithm starts finding minimum spreading gain for the network and individual transmission powers for all transmitters in the network following the above optimisation problem. If spreading gain of the optimisation problem results lesser than some positive value then all nodes can transmit at the same time, otherwise the first node to be eliminated from transmission is the transmitter closest to any receiver other than its intended receiver. Elimination of this transmitter receiver pair will decrease the required spreading gain. This loop with the algorithm will be executed unless a set of transmitter receiver pair is found where the spreading gain upper limit is satisfied. All eliminated nodes will be considered for the next consecutive time slots. As a result all transmitter receiver pairs in the network will be divided into different subset and nodes in each subset will transmit in one time slot with spreading gain less than some positive value.

This algorithm could be invoked at the beginning of every time slot in order to cope with the interference level or at the end of all transmitters from all subset finishes transmission. Theoretically the later gives the optimal solution. The invocation time of this algorithm is very important. Let us first consider that a set of n nodes is divide into m subsets according to the Scheduling-Spreading gain. These m subsets will transmit in m consecutive time slots. Hence, The results of the algorithm is true and optimum if within m consecutive time slots no other new transmitters are considered. In other words this result is true for m consecutive time slots and within this period no mobility, addition or deletion of nodes are considered within the network. So, let us concluded that if this algorithm is invoked at the end of m time slots, minimum total network energy is consumed but not a realistic solution in terms of mobile ad hoc network. It is much realistic to assume that this algorithm is invoked at the beginning of every time slot with the assumption that interference level at each receiver remains constant during one time slot. In this case this algorithm will find a subset from all transmitters to transmit in the next time slot, where spreading gain is less than some positive value. Mobility, addition and deletion of nodes could be taken into account at the beginning of every time slot. This ensures realistic approach, but lacks of fair scheduling. This means that a node may not get a chance to transmit at all because of new set with k nodes are formed within the network.

C. Optimized Encryption and Decryption Scheme (OEDS)

In this phase, both encryption and decryption schemes are implemented. Here three types of iterations are used while converting plaintext to ciphertext. In first iteration, plaintext is converted into ASCII value. In second, ASCII is converted into BCD value. In third, BCD is converted in to Hexadecimal value.

The following cryptographic primitives are used in PSEC:

1. KDF is a key derivation function that is constructed from a hash function.

2. ENC is the encryption function for a symmetric-key encryption scheme such as the AES, and DEC is the decryption function.
3. MAC is a message authentication code algorithm such as HMAC.

Encryption phase

```
INPUT: Domain parameters $D$ = $(q$,FR, $S,p,q, P,n,h)$, public key $Q$, plaintext $m$.
OUTPUT: Ciphertext $(R,C, s, t)$.
1. Select $r$ ∈$R$ {0,1}$l$, where $l$ is the bitlength of $n$.
2. $(k', k1, k2)$←KDF$(r)$, where $k'$ has bitlength $l$ +128.
3. Compute $k = k'$ mod $n$.
4. Compute $R = kP$ and $Z = kQ$.
5. Compute $s = r$ ∈ KDF$(R, Z)$.
6. Compute $C$ = ENC$k1(m)$ and $t$ = MAC$k2$ $(C)$.
7. Return$(R,C, s, t)$.
```

Decryption phase

```
INPUT: Domain parameters $D$ = $(q$,FR, $S,p,q, P,n,h)$, private key $d$, ciphertext $(R,C, s, t)$.
OUTPUT: Plaintext $m$ or rejection of the ciphertext.
1. Compute $Z = dR$.
2. Compute $r = s$∈ KDF$(R, Z)$.
3. $(k\_ , k1, k2)$←KDF$(r)$, where $k\_$ has bitlength $l$ +128.
4. Compute $k = k'$ mod $n$.
5. Compute $R' = kP$.
6. If $R'$ = $R$ then return("Reject the ciphertext").
7. Compute $t' =$ MAC$k2(C)$. If $t\_$ = $t$ then return("Reject the ciphertext").
8. Compute $m$ = DEC$k1(C)$.
9. Return($m$).
```

Proof for Decryption: If ciphertext (R,C, s, t) was indeed generated by the legitimate entity when encrypting m, then $dR = d(kP) = k(dP) = kQ$. Thus the decryptor computes the same keys $(k', k1, k2)$ as the encryptor, accepts the ciphertext, and recovers m.

D. Proposed packet format

Source ID	Destination ID	Authentication Status	Scheduling Status	Energy Conservation Rate	CRC
1	1	3	3	4	1

Figure 1..Proposed Packet Format

In figure 1. the proposed packet format is shown. Here the source and destination node ID carries 1 byte. Third one is authentication status of the node. The authentication status induces the whether the transmission of packets are travelled through authenticated route. In fourth field, the scheduling status is indicated. It determines how much of the genuine packets are transmitted based on the time slot. It also determines whether packet contains authorized information. In fifth, the energy conservation ratio is allotted to ensure minimum energy consumption. The last filed CRC i.e. Cyclic Redundancy Check which is for error correction and detection in packet while route maintenance process.

The flow diagram of the proposed scheme is show in figure 2. In this scenario, each mobile node communicates through the neighbor mobile nodes while integrating with cross layer framework. The encryption and decryption scheme is also deployed in each and every packet from source to destination. This makes packet with higher data integrity and to identify the authenticated mobile destination node or source node.

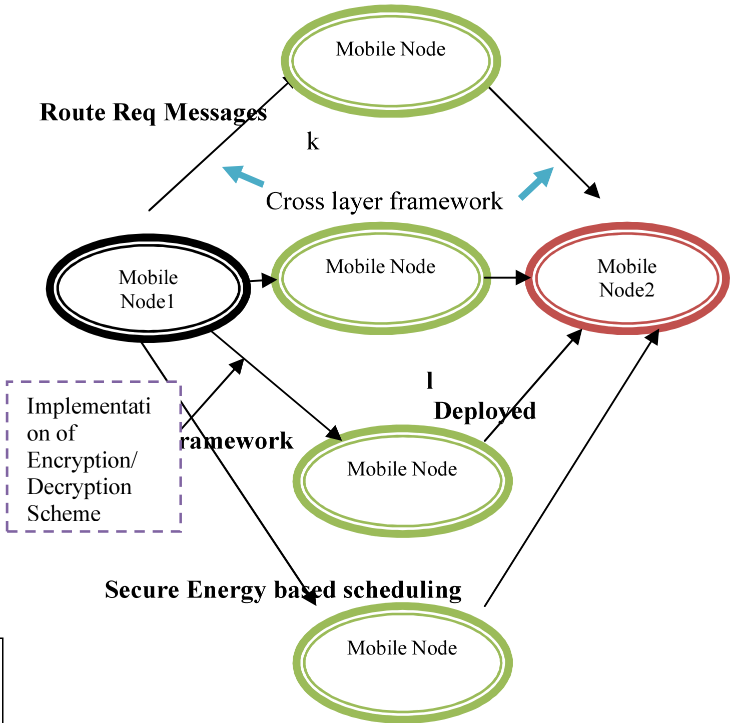

Fig.2. Flow Chart Of Proposed Scheme

4. PERFORMANCE EVALUATION

The proposed scheme is simulated with the AODV protocol. The Network Simulator (NS 2.34) is used to simulate our proposed algorithm. In our simulation, 101 mobile nodes move in a 1100 meter x 1100 meter square region for 120 seconds simulation time. All nodes have the same transmission range of 300 meters. The simulated traffic is Constant Bit Rate (CBR) and Poisson traffic. Our simulation settings and parameters are summarized in table 1.

A. Performance Metrics

We evaluate mainly 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.

Table1. Simulation Settings And Parameters

No. of Nodes	101
Area Size	1100 X 1100
Radio Range	300m
Simulation Time	120 sec
Traffic Source	CBR and Poisson
Packet Size	512 bytes
Mobility Model	Random Way Point
Pause time	5 msec
Packet Queuing	Drop Tail
Protocol	AOMDV

The simulation results are presented in the next part. We compare our CSCAS with the CDJPCSA [16] and USOR protocol [17] in presence of Scheduling and Security environment.

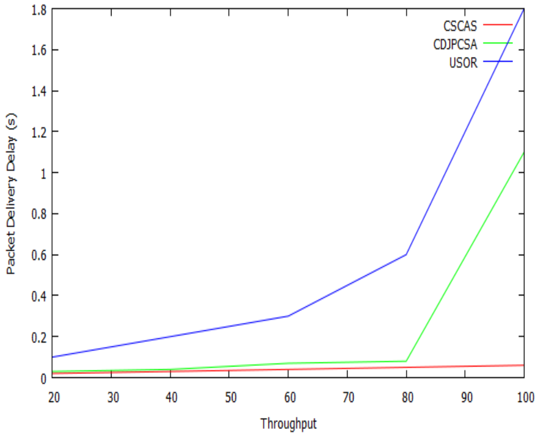

Fig. 3. Throughput Vs Packet delivery delay

Figure 3 showshe results of packet delivery delay for varying the throughput from 10 to 100. From the results, we can see that CSCAS scheme achieves low delay than the USOR and CDJPCSA schemes because of scheduled routing.

Figure 4 shows the results of packet delivery ratio for varying the nodes from 10 to 100. From the results, we can see that CSCAS scheme has higher delivery ratio than the USOR protocol and CDJPCSA schemes.

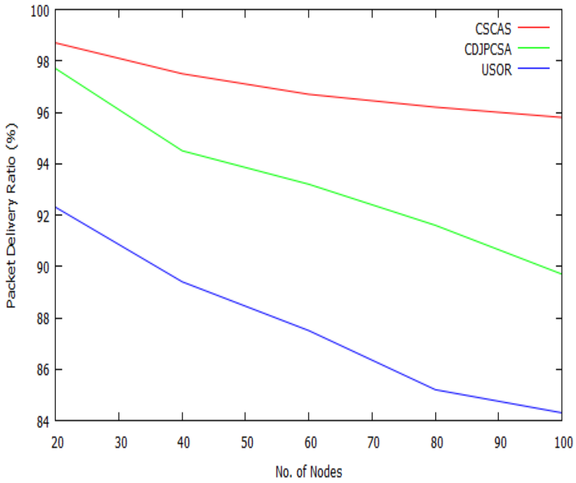

Fig. 4. No. of Nodes Vs delivery ratio

Fig. 5, presents the comparison of overhead and mobility. It is clearly shown that the overhead of CSCAS has low overhead than the CDJPCSA and USOR protocol.

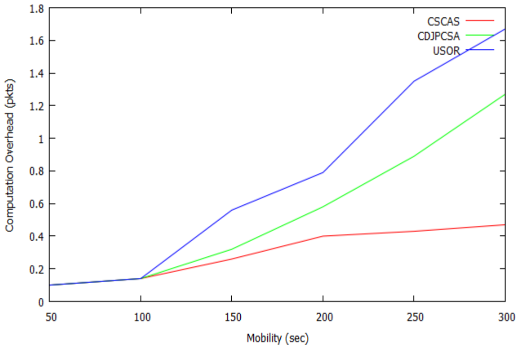

Fig. 5. Nodes Vs Overhead

Figure 6 shows the results of Simulation time Vs Network Lifetime. From the results, we can see that CSCAS scheme has higher Network Lifetime than the USOR protocol and CDJPCSA while varying the simulation time 10 to 50.

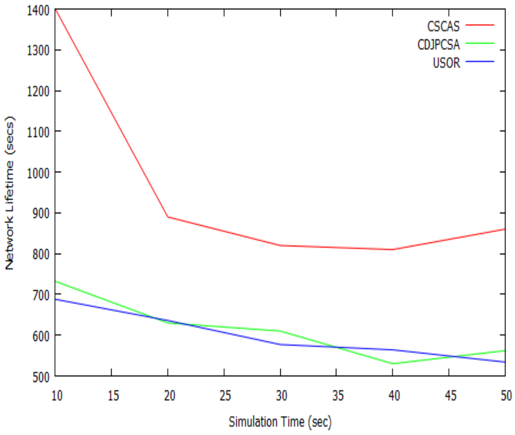

Fig..6. Simulation Time Vs Network Lifetime

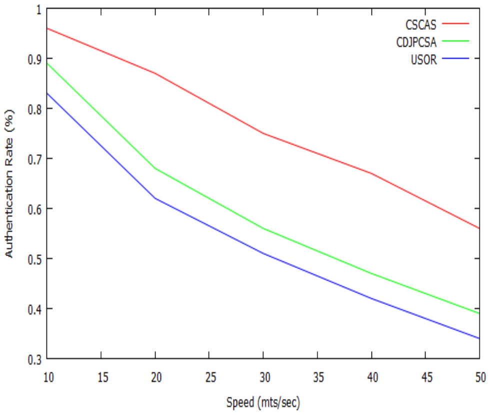

Fig. 7. Speed Vs Authentication Rate

Figure 7 shows the results of Speed Vs Authentication Rate. From the results, we can see that CSCAS scheme has higher Authentication rate than USOR protocol and CDJPCSA while varying the speed from 10 to 50.

5. CONCLUSION

Mobile nodes are moving randomly without any centralized administration in MANET. Due to high mobility the packet loss occurs unnecessarily and the integrity of the packet is not genuine. In the presence of the attacks, the data is collapsed or damaged. In this paper, we have developed a Cross Layer frame work with security and scheduling mechanism for Authentication which attains the integrity and reduced congestion among nodes. In the first phase of the scheme, Cross Layer design is proposed. Here the information is sent to the source node depends upon the fading of channel determined from destination node. In second phase, scheduling algorithm with CDMA is proposed to achieve scheduling status and time slot allocation. In third phase, the Optimized Encryption/ Decryption Scheme is proposed to achieve high integrity and authentication. In future work, the energy consumption of mobile nodes will be minimized using the energy consumption model with delay approach. By using the extensive simulation results, the proposed scheme CSCAS achieves the better packet delivery ratio, authentication rate, scheduling rate, low packet delivery delay and overhead than the existing schemes namely USOR and CDJPCSA while varying the mobility, simulation time and number of nodes.

REFERENCES:

[1] Asmidar Abu Bakar , Roslan Ismail , Abdul Rahim Ahmad and Jamalul-Lail Abd Manan, “Ensuring Data Privacy and Security in MANET: Case in Emergency Rescue Mission”, *International Conference on Information and Knowledge Management*, 2012, pp.165-169.

[2] 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.

[3] Djallel Eddine Boubiche and Azeddine Bilami, “Cross Layer Intrusion Detection System for Wireless Sensor Network”, *International Journal of Network Security & Its Applications (IJNSA),* Vol.4, No.2, March 2012, pp.35-52.

[4] Rekha Patil , Dr.A.Damodaram, “ Cost Based Power Aware Cross Layer Routing Protocol for MANET”, *International Journal of*

Computer Science and Network Security, Vol.8 No.12, December 2008, pp.388-393.

[5] Kazuya Nishimura and Kazuko Takahashi, "A Multi-Agent Routing Protocol with Congestion Control for MANET", *European Conference on Modelling and Simulation,* 2007, pp.1-6.

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

[7] Qi Qu, Laurence B. Milstein, Fellow IEEE, and Dhadesugoor R. Vaman, Senior Member, IEEE, "Cross-Layer Distributed Joint Power Control and Scheduling for Delay-Constrained Applications over CDMA-Based Wireless Ad-Hoc Networks", *IEEE Transactions On Communications,* Vol. 58, No. 2, February 2010, pp. 669-680.

[8] L. Krishna Bharathi and Gnanou Florence Sudha, "Security Enhancement Using Mutual Authentication in Existing CDMA Systems", *International Journal on Computer Science and Engineering* Vol. 02, No. 02, 2010, pp.237-245.

[9] E. Sousa and J. A. Silvester, "Spreading code protocols for distributed spread-spectrum packet radio networks," *IEEE Trans. Commun.*, pp. 272–281, Mar. 1998.

[10] H.-L. Chao and W. Liao, "Fair scheduling with QoS support in wireless ad hoc networks," *IEEE Trans. Wireless Commun.,* vol. 3, pp. 2119– 2128, Nov. 2004.

[11] S. Ramanathan and E. Lloyd, "Scheduling algorithms for multihop radio networks," *IEEE/ACM Trans. Networking*, vol. 1, pp. 166–177, 1993.

[12] H. Sui, E. Masry, and B. D. Rao, "Chip-level DS-CDMA downlink interference suppression with optimized finger placement," *IEEE Trans. Signal Process.,* vol. 54, no. 10, pp. 3908–3921, Oct. 2006.

[13] Shan-shan Ma and Jian-sheng Qian, "Location-Unaware Node Scheduling Schemes Based on Boundary Nodes in Wireless Sensor Networks", *Przegląd Elektrotechniczny,* Vol. 89, 2013, pp.71-74.

[14] Jing Deng, Yunghsiang S. Han,, Wendi B. Heinzelman and Pramod K. Varshney, " Balanced-energy sleep scheduling scheme for high-density cluster-based sensor networks", *Elsevier, Computer Communication,* Vo.28, 2005, pp.1631-1642.

[15] 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.

[16] Sandeep Sharma, Rajesh Mishra, Karan Singh, "Current Trends and Future Aspects in Cross layer Design for the Wireless Networks", *Computer Science & Information Technology (CS & IT)*, 2012, pp.283-296.

[17] Zhiguo Wan, Kui Ren, and Ming Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks", *IEEE Transactions on Wireless Communications,* Vol. 11, No. 5, May 2012, pp.1922-1932