**I J C T A**, 9(2) 2016, pp. 531-545


# Efficient Authentication based IP Configuration for MANETS using Elliptic Curve Digital Signature Algorithm

**[1]Hemamalini V., [2]Zayaraz G. and [3]Vijayalakshmi V.**

**ABSTRACT**

For connecting into the internet world IP configuration is an important requirement in Mobile Ad Hoc Network (MANET). Hence, before involving in any sort of communication each node inside MANET should be self-configured yielding maximum performance metrics. To attain this each end terminal within the MANET network should be configured with a unique IP address. There have been several existing IP addressing schemes that adds complexities to the network, which shows results only in average latency and low communication overload. Apart from latency and overhead, performance metrics like throughput, delay and packet delivery ratio are important to qualitatively analyze a good addressing scheme metrics. Hence, the above metrics have not been discussed in detail till date. This paper proposes a certificate integrated IP allocation mechanism that uses an authentication based IP configuration utilizing Elliptic Curve Digital Signature Algorithm (ECDSA) that defends the security issues and improves the performance metrics.

***Keywords:*** MANET; Multi-hop routing certificate; dynamic address scheme; Elliptic Curve Digital Signature Algorithm (ECDSA); Elliptic Curve Cryptography (ECC).

## 1. INTRODUCTION

MANET is a self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Due to limited transmission range, battery power and bandwidth it requires multiple hops to exchange data between nodes. Before any communication starts , each node inside Manet should be identified mutually, in particular, they need to be addressed uniquely. With the help of a certain routing protocol namely AODV, nodes inside Manet should be configured with a unique address for routing of packets to be destined to the correct location. In wired networks for allocation of static or dynamic IP Dynamim Host Configuration Protocol(DHCP)[1] is used.For unique address allocation, MANETs has gained more examinations, for which performance metrics should be analysed. This has led to an increase in the significance of the process of assigining unique IP addresses in Manets.In turn this results in successful adaptation of the Manets to scalability,robustness and security.Thus a node without IP configuration should be able to configure itself within a given time,devoid of exessive network or/and communication overhead in addition to best throughput,low latency and packet delivery ratio.Also a node in Manet has the tendency to depart from its network during which its IP can be claimed for future.There is always a possibility of the node to join later, and hence all these conditions should be well stuctured for distributed and unpredictable nature of Manets.

[1] Research Scholar, Department of Computer Science & Engineering, Pondicherry Engineering College, Pondicherry, India
[2] Professor, Department of Computer Science & Engineering, Pondicherry Engineering College, Pondicherry, India
[3] Assistant Professor, Department of Electronics and Communication Engineering, Pondicherry Engineering College, India
*E-mail: cse.malini@gmail.com, gzayaraz@pec.edu, vvijizai@pec.edu*

Any addressing schemes developed for MANET should achieve the following objectives:

**(i) Dynamic IP Configuration:** Without user intervention nodes should be able to get an IP address.

**(ii) Uniqueness:** No address conflict should occur and hence address should be unique.

**(iii) Robustness:** System should consider network partitioning and scheduling.

**(iv) Scalability:** As the size of the network increases the system should be fault tolerant against the network size. Therefore, in the case of joining a new node, each node sends (x-1) messages and receives (x-1) messages if the total number of nodes in the network is x. Therefore, flooding occurs, due to which the communication complexity becomes O ((n -1) × (n-1))), that is O ($n^2$)

**(v) Security:** Security threat is also an issue during address allocation since authentication needs to be carefully verified; else several security threats can arise.

## 2. RELATED WORK

This section describes about the primary address allocation strategies and also describes its disadvantages.

The various addressing plans [2, 3] for ad hoc networks are classified into 3 broad categories viz.,

- Best Effort Allocation.
- Leader Based Allocation.
- Decentralized Allocation approaches.

In the first method (i.e.) each node allocates its own IP without the supervision of other nodes. The best example is the Prophet scheme which allocates addresses using random number generation. Here addressing latency and communication overhead is low which creates a lot of advantage. Despite the huge location space, there are chances of address conflicts, which can be handled using passive or weak DAD [19].

In the second method (i.e.) DAD mechanism is eliminated by choosing legitimate IP's from a chosen pioneer or server of the system. This is exemplified in the following:

(i) DHCP [4] - This requires broadcasting of messages for discovering a server.

(ii) DACP [5] - This scheme produces high overhead.

(iii) VASM [2, 6] - The use of zero knowledge proof states only that the statement is true but not the information.

(iv) Lightweight secure address configuration scheme [2, 7].

In the third method (i.e.) decentralized designation, guarantees uniqueness of location. Here, an IP is obtained either by its own or from its neighbor and then the DAD mechanism is performed. Few examples are (i)MANETconf [8] (ii)AAA [21] (iii)Prime DHCP [9] (iv)AIPAC [10] (v) Secure host auto-configuration plan [11] (vi)Quadratic residue based location allotment [12] (vii)Secure auto-arrangement plan [13] (viii)MMIP [14] (at the time of location allocation, every node in the system acts as proxies and ties the MAC address with the IP address) (ix)ADIP [15] (IP addresses are generated from its own particular IP for another verified host with the concept of proxies) (x)IDDIP and IDSDDIP algorithm [16,17] (ID mechanism is used).

The above schemes exhibit certain disadvantages such as usage of DAD, complexity in implementation, authentication handled by third party which becomes a security threat. The latest mechanisms of Ghosh and Uttam states that, the use of RSA public key technique results in average latency and communication overhead.

## 3. PROPOSED CI-ECDSA MECHANISM

Generally nodes in MANET communicate with one another within a given network. However,communication fails when the nodes are out of range.Hence many security issues arises due to which performance gets degraded.

This proposed work is referred to as Certificate Integrated Elliptic Curve Digital Signature Algorithm (CI-ECDSA) addressing scheme. This paper proposes a method in which X.509 certificate is utilized for client authenticity which is the fundamental issue in MANET. In the current IDDIP plan, RSA is utilized as an open key framework that increases latency and communication overhead. For Signature generation and verification this technique utilizes Elliptic Curve Digital Signature Algorithm (ECDSA), a variation of Digital Signature Algorithm (DSA) which utilizes Elliptic Curve Cryptography (ECC) implanted as a part of the declaration. With the examination considered from the paper [18, 20], authentication incorporated with ECC shows improved results over RSA which substantiates the fact that ECC is better than RSA. The architectural view of CI-ECDSA addressing scheme is depicted in the following Figure 1.

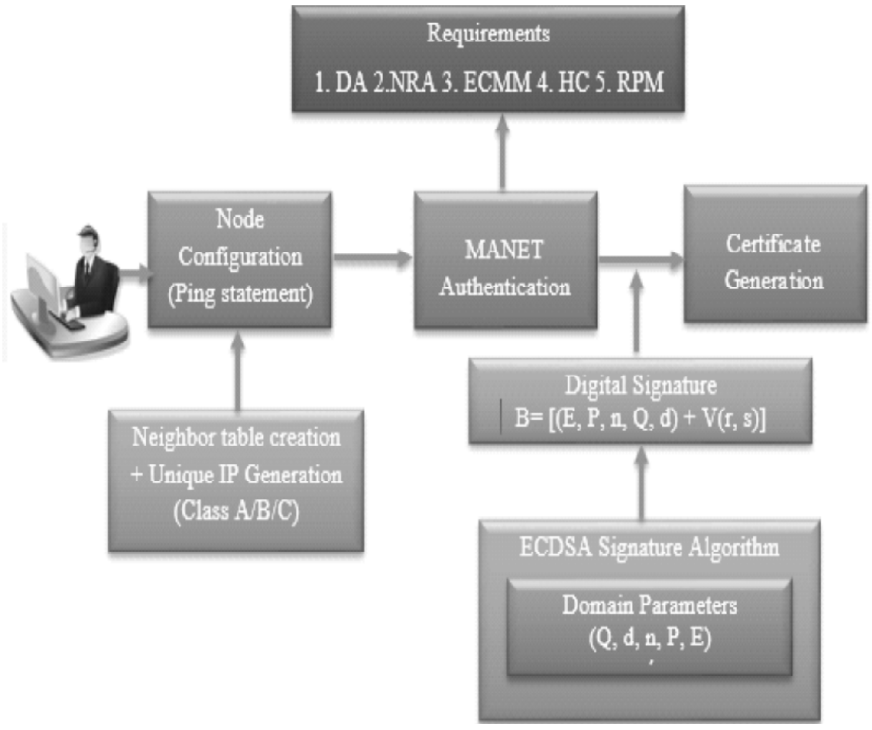


**Figure 1: Architectural view of CI-ECDSA Addressing mechanism**

The different stages of the CI-ECDSA mechanism are illustrated in Figure 2, and the explanation of each stage is given as follows:

### 3.1. Node Configuration

A neighbor table is created with the help of ping statement during the node formation stage. This process involves configuration of IP address and generation of certificate. At this stage all the nodes are identified by its configured IP.

### 3.2. Authentication

In a MANET, the cluster based network has been used for efficient authentication process. It is provided by the Certificate Authority (CA), a trusted third party that contains information about all the nodes in the

network. Generally, the node in the cluster environment is specifically formed by Cluster Based Routing Protocol (CBRP). It provides an efficient routing process between the nodes. Each node communicates with other through one-hop monitoring. One hop monitoring contributes for communication between one nodes to other.

### 3.3. Requirements for Authentication

The following are the requirements for authentication process in MANET:

(i) **Distributed Authentication:** Validation among the set of nodes in a network is an essential requirement for certificate based authentication.

(ii) **Resource Awareness:** The protocol utilized must be proficient both as a part of memory and power.

(iii) **Efficient Certificate Management Mechanism:** Dealing with the certificates (formation, revocation, and regeneration) and applying these techniques to MANETs, is a testing issue. In this way the certificate should be managed in the ad hoc system to give an effective communication and to deal with the nodes in the system.

(iv) **Heterogeneous Certification:** In Wireless Network, the guaranteeing powers may be heterogeneous even in specially appointed systems. This implies that two or more nodes fitting in with diverse "domains" may attempt to validate one another. In such cases, there must be a trust relationship or chain of command.

(v) **Robust Pre-Authentication Mechanism:** In this mechanism, the methodology making vital trustbetween nodes before the genuine declaration creation and appropriation is carried out. This mechanism is mandatory, since it is an efficient way for the nodes to furnish a former trust with one another.

### 3.4. Certificate Generation

The certificate based authentication in MANET requires undergoing the following steps:

(i) The certificate has been signed by a trusted CA.

(ii) Checks the validation of the certificates.

(iii) Checks whether the certificate has been revoked. Checks the proof possession of the client.

The Certificate Authority (CA) in mobile network is neither fixed nor centralized. Rather, it provides a mobility mechanism for the data communication between the nodes in the wireless network. Thus, the CA is the trusted third party which contains all the information about the other nodes in the network like the ID, serial number, transmission range, and the like. Before nodes can join the system, they need to gain legitimate certificates from the CA. It is the role of the CA for overseeing and appropriating certificates of all nodes with the goal that nodes can speak with one another enormously in a MANET.

To empower every versatile node to preload the certificate, Certification Authority, is conveyed in the system. The CA is additionally in charge of revocation of nodes in the system and therefore retains all the alternate nodes in the system.

### 3.5. Steps in Certificate Authentication

**Step 1:** Initialize the node in the network to process the function effectively.

**Step 2:** Assign any node as CA which must contain information about the other nodes in the network.

**Step 3:** Each node has a certificate which contains the public key (Common Key), own id, transmission range etc.

**Step 4:** Transferring information between the nodes in the network to form a group which contains each node has a valid certificate.

**Step 5:** Check the validity of the certificate of the nodes by broadcasting an alert message to another group of nodes by the CA with the same transmission range.

**Step 6:** If any revocation or creation of node is in process inside the network, it must be updated in CA.

**Step 7:** During communication, the information is passed through the other node confidentially by authentication using information provided on the certificate.

**Step 8:** If the authentication parameter is not equal with the CA, then the corresponding node is neither neglected nor represent as unauthorized node.

**Algorithm 1. Address Allocation for New Node**

When a new Node $n_i$ is arrived to join a network.

NC = Node Count
NIP = Node IP
NId = Node ID
NC=0;

1. **if** NC==0 **then**
   // generate random IP
2. NIP=RIP Generation ();
3. NId=1;
4. NC=NC+1
5. **else**
6. Generate pubKey, privKey using ECDSA algorithm
7. Generate Sig (pubKey, REQ)
8. **while** (flag=true)
9. Broadcast REQ msg neighbors
10. **if** (timeout) **then**
11. flag=false;
12. **end**
13. **end while**
14. **if** $n_i$ receives multiple RES from other Nodes **then**
15. **for** (i=1; i<RES.length; i++)
16. Select short range (Communication) Node
17. **end for**
18. NC=NC+1
19. NId=NC;
20. Extract IP from RES message
21. Generate Sig (pubKey, NId, NIP, ACK)
22. Broadcast ACK to neighbors.

23. Receive ACK_RES
24. **else**
25. **Goto** Step 6
26. **end**
27. **end**

When a new node arrives the Node Count is checked. If it is the first node, it enters into a network and a random IP is generated using RIPGeneration (). The IP address is classified as Class A, Class B and Class C. Each class contains a unique range of IP address. If Class A is selected, then the IP range is 1.0.0.0 to 127.255.255.255. If Class B is selected, then the IP range is 128.0.0.0 to 191.255.255.255. If Class C is selected, then the IP range is 192.0.0.0 to 255.255.255.255.The initial value of IP is set between 0-255.The node selects the class after generate IP () from the class range.

For the first node, Node id=1, for the second node and other nodes following it Node id =NC. When this node id is not equal to 0, then the node creates a public, private key pair using ECDSA algorithm. The node generates the Signature with public key as REQ for requesting IP allocation. The generated Signature request is broadcasted to all neighbors in the network. A particular time is fixed for broadcasting and hence if timeout is reached the message is stopped.

Once the REQ message is received by all the nodes in the network, signature verification is done. If it is true, then the IP is assigned to the new node by the node which belongs to the particular class. The received node calls generateIP () method to generate the unique IP. The generated unique IP is sent to the requester. The new node receives multiple unique IP address from the neighbors. The selection of the particular node that has given RES (IP Allocation) out of all other nodes is selected by short range communication node.

**Algorithm2. When a Node Receives REQ**

1. **If** $n_i$ receives REQ then
2. Boolean b=VerifySig ();
3. **if** (b) // true
4. CLS=Extract IP Address Class
5. x=getStartRange ()
6. y=getEndRange ()
7. IP=**generateIP(x, y);**
8. Send RES (IP) to Node
9. **end**
10. **end**

**Algorithm3. Function RIPGeneration ()**

CLS=Class

RIP = Generated IP address

Set i=0, j=0, k=0

1. Randomly Select any CLS (A || B || C)
2. **if** CLS==A

Select IP address from the range of 1.i.j.k to 127.255.255.255

f=random (1,127);
i=random (0,255);
j=random (0,255);
k=random (0,255);
RIP=f.i.j.k
**return** RIP

3. **else if** CLS == B
   Select IP address from the range of 128.i.j.k to 191.255.255.255
   f=random (128,191);
   i=random (0,255);
   j=random (0,255);
   k=random (0,255);
   RIP=f.i.j.k
   **return** RIP
4. **else** // CLS=C
   Select IP address from the range of 192.i.j.k to 255.255.255.255
   f=random (192,255);
   i=random (0,255);
   j=random (0,255);
   k=random (0,255);
   RIP=f.i.j.k
   **return** RIP

**Algorithm4. Function GenerateIP(x, y)**

1. Set p=x; q=y; j=0; k=0; l=0;
2. Select IP
   i=random (p, q);
   j=random (0,255);
   k=random (0,255);
   l=random (0,255);
3. IP=i.j.k.l;
4. **return** IP;
5. **else**
6. call generateIP ()

### 3.6. ECDSA Authentication in MANET

Domain Parameters:

Q – Public key
d – Private key
n – No.of.nodes

P – Prime no. for calculation

E - Concerned nodes authentication entity

(i) CA contains information's about all the intermediate nodes. Certificate generation has public key and a private key to communicate between nodes. Therefore, for generating a public and private key,

A = (E, P, n, Q, d) respectively….. (1)

(ii) Generating a signature standard for the certificate requires a secure hash algorithm.Therefore Signatures for message M is

M = (r, s)…..…… (2)

Were r ≠ null & s ≠ null from the above derived equation.

(iii) Verifying the signatures of the message M = (r, s) that denotes = r…….…….. (3)

were V – Certificate Authority (CA) and r – Message

(iv) The proposed ECDSA authentication by the user B verifies A's Signature values in order to communicate the information.

From **1, 2 & 3**, the proposed authentication scheme is,

B = [(E, P, n, Q, d) + V(r, s)]

## 4. RESULTS AND DISCUSSIONS

### 4.1. Performance Metrics

Some of the performance metrics compared with the proposed CIECDSA address allocation plan with other existing plans are as follows:

(i) Packet Delivery Ratio: The degree of the quantity of conveying information bundle to the goal. This represents the level of conveyed information to the terminus.

(Σ Number of bundles received/ Σ Number Of bundles Sent)

(ii) Delay: The normal time taken for an information packet to land at the destination. Likewise it incorporates the delay caused by route discovery process and the queue line in the information packet transmission.

(Σ (Arrive Time – Send Time)/ Σ Number of Associations)

(iii) Latency: Latency can be described as the duration of time between an IP requests and assigning of IP by a node in a system. Shorter latency will be guaranteeing better protocol.

(iv) Communication Overhead: Communication overhead is those bits of data that must be sent to convey information about, for example, where the information originated and where it is being sent to, how it is to be routed, timestamps, or any other information that is not actually the "payload" representing the actual content to be communicated.

(v) Throughput: Throughput or network throughput is the rate of successful message delivery over a communication channel.

### 4.2. Performance Comparison

Table 4.1 & 4.2 demonstrates the near investigation of the current and proposed plans. The investigation is been centered on subjective assessment of all methodologies. The values are as underneath:

n- No. of versatile nodes in the network

t- Average 1-hop latency

d- Width of network

p & c- Complexity of public key Digital Signature of existing algorithm

**Table 4.1**
**Qualitative comparison of performance metrics of various existing approaches with proposed CIECDSA scheme**

| *Metrics* | *MMIP* | *ADIP* | *IDDIP* | *IDSDDIP* | *CIECDSA* |
|---|---|---|---|---|---|
| Uniqueness | Yes | Yes | Yes | Yes | Yes |
| Latency | O (2t) | O(2t+m) | O (2t+p) | O (2t+p+c) | O(t) |
| Overhead | O (n/2) | O (n/2) | O (n/2) | O (n/2) | O(n-1)/2 |
| Complexity | Low | Low | Low | Low | Low |
| Periodic Message | No | Yes | Yes | Yes | Yes |
| Security | Yes | Yes | Yes | Yes | Yes |

**Table 4.2**
**Comparison of performance metrics values of various existing schemes with the proposed CIECDSA scheme**

| *Metrics* | *MMIP* | *ADIP* | *IDDIP* | *IDSDDIP* | *CIECDSA* |
|---|---|---|---|---|---|
| Latency | 0.32 ms | 0.30 ms | 0.25 ms | 0.21 ms | 0.17ms |
| Overhead | 10 ms | 7 ms | 5 ms | 4 ms | 1.5 ms |
| Throughput | 72% | 75% | 78% | 85% | 88% |
| Delay | 30 ms | 28 ms | 20 ms | 12 ms | 7 ms |
| Packet delivery Ratio | 68% | 70% | 72% | 80% | 96% |

The latency for the different IP mechanism developed by Raj and Uttam such as MMIP, ADIP, IDDIP and IDSDDIP exhibits the following complexity values such as 2t, 2t+m, 2t+p, 2t+p+c respectively. In this the variables m, p & c is recognized as the intricacy of the encryption/decryption algorithms plus the public key Signature (RSA algorithm). Henceforth the latency describes the complexity that occurs in the last three strategies. The overhead in communication is calculated as the normal degree (n/2) for each node in the system.

The proposed plan gives authentication to address set up while dealing with the security issues utilizing Elliptic Curve Cryptography (ECC). Accordingly, to lessen the latency and overhead and to draw out an effective throughput the proposed is presented by X.509 authentication with ECC incorporated in IPv4 addressing scheme. In the proposed CIECDSA execution investigation shown in table 4.1, the latency and communication over head is O (t) and O (n-1)/2 respectively. In table 4.2 the various values for the different performance metrics have been computed and displayed with the comparison to the proposed CIECDSA, which clearly states that the proposed is best.

### 4.3. Simulation Parameters

To analyze the execution of the proposed CIECDSA plan with some comparable existing procedures IDDIP and IDSDDIP has been compared with the proposed CIECDSA system. Due to low communication overhead and less tending to latency IDDIP and IDSDDIP scheme is selected and contrasted with the other mainstream existing plans. IDDIP utilizes a conventional hash function for node authentication and RSA as the public key digital Signature for the message authentication system. In spite of the fact that IDDIP can oppose false

reply attack from a malevolent hub, the cryptographic algorithm builds the latency for address allocation. In this proposed mechanism, CIECDSA demonstrated great execution results regarding latency and throughput. The simulation is carried out utilizing a NS-2 simulator installed in Ubuntu (in existing Oracle VM Virtual Box Manager). Performance metrics such as throughput, packet delivery ratio, delay, latency, and communication overhead are chosen as the execution measurements and the outcomes are exhibited under simulation results.

**Table 4.3**
**Parameter used in simulation**

| | |
|---|---|
| Simulation Time | 15s |
| Protocol | Modified AODV, 802.11 (MAC Layer Protocol) |
| Number of Nodes | 50 Nodes |
| Map size | 1000m x 1000m |
| Mobility model | Random Walk |
| Traffic type | Constant Bit Rate (CBR) /UDP |
| Transmission range | 15m |
| Packet size | 512 KB |
| Connection rate | 200 Mb/s |
| Connections | 5s |
| Pause time | 0.05s |
| Maximum Node Speed | 0 to 15ms |

Table 4.3 demonstrates the simulation parameters that have been used. To check the accuracy of the simulation process, a system comprising of 50 hubs is created. Radio transmission scope of every hub is situated at 15 m. For ad hoc routing protocol modified AODV is used for routing of packets. For Medium Access Control (MAC), 802.11 have been used as the link layer protocol. UDP protocol is utilized for transport layer. Likewise, Constant Bit Rate (CBR) traffic generator is being utilized for a bundle size of 512kb at the rate of 1mbps. A hub joins the MANET each 15 s.

In the IDDIP mechanism, address allocation, is done through single hop broadcast, but CIECDSA requires each and every hub to keep trade of data with different nodes in the gathering it fits in with. It then acquires the public keys by staying informed. Additionally, every hub keeps a trust table for storing trust values of different nodes. Figure 2 to Figure 6 demonstrate the quantity of bundles received from each of the nodes in the network crosswise over time. When simulated it is seen that CIECDSA increases in throughput and packet delivery ratio and reduces in case of delay. This checks the rightness of the simulation process.

### 4.4. Simulation Results

The simulation performed under static scenario is shown in this subsection. The throughput, packet delivery ratio, delay, communication overhead and the addressing latency for the five schemes (CIECDSA, IDSDDIP, IDDIP, ADIP and MMIP) is assessed under thought and the outcomes have been compared.

(a) Throughput Ratio: Throughput demonstrates the measure of computerized information transmitted per unit time from source to destination. Figure. 2 shows the average throughput plotted with time against the number of packets. It is noted that the throughput for CIECDSA is high compared to the other four existing schemes. The increase of throughput compared to existing IDSDDIP, IDDIP, ADIP and MMIP are 3%, 10%, 13% and 16% respectively. This exhibits large IP addressing scheme. Within certain time period the throughput varies are noted between the four existing schemes and the variation was observed among them.

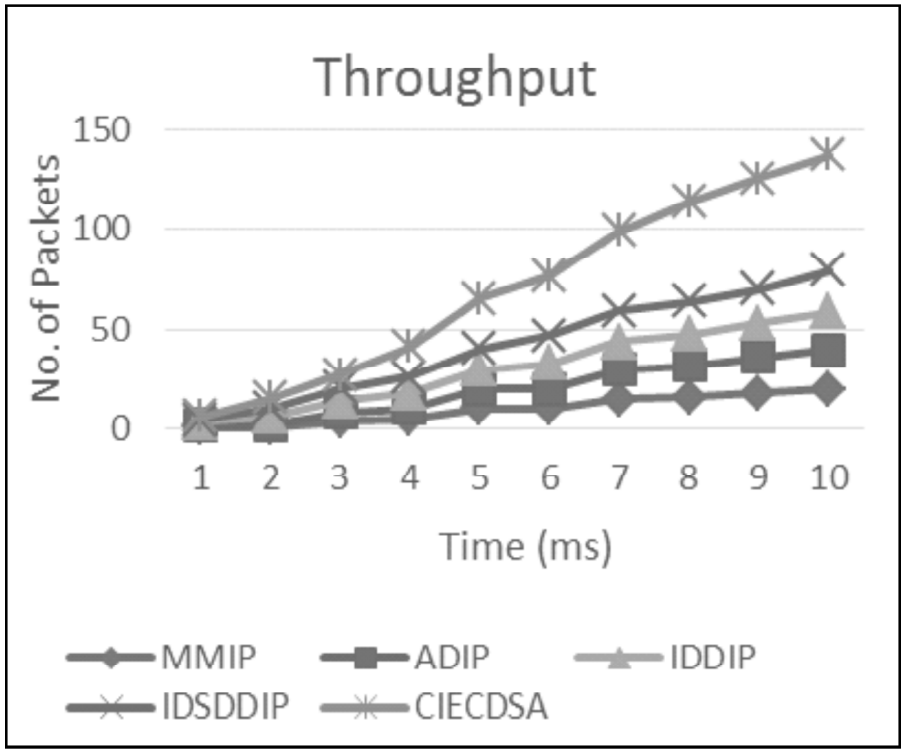


**Figure 2: Throughput Ratio**

(b) Packet Delivery Ratio: The part of the information packets conveyed to destination hubs sent by source hubs is defined as packet delivery ratio. Figure. 3 show that as the throughput increases the packet delivery ratio for the proposed CIECDSA scheme gets increased. The percentage of CIECDSA improvement compared to existing IDSDDIP, IDDIP, ADIP and MMIP are 16%, 24%, 26% and 28% respectively.

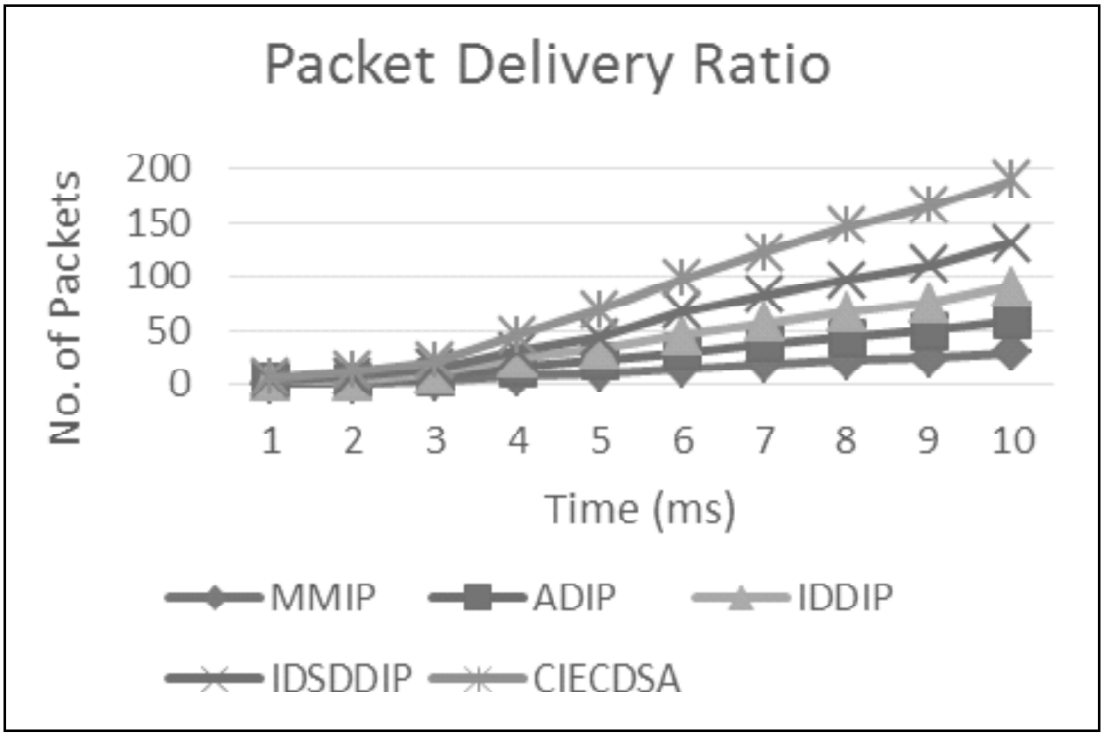


**Figure 3: Packet Delivery Ratio**

(c) Packet Delay: Delay is the average time taken by the information bundles from source to destination, and it includes buffer and lining delays during route discovery and interface queues respectively. Retransmission delays also occur at the MAC layer and propagation time. This metric is measured by plotting the time over number of packets and the result shows that as the time increases, the delay level in CIECDSA is low to certain level and gets saturated after a certain level, compared to that of other four schemes that shows an increase in delay. As shown in Figure 4 the CIECDSA exhibits the lowest level bar curve, where initially both CIECDSA and IDSDDIP starts at the same point and then shows the difference in the bar. The difference in delay when compared to CIECDSA is 5ms, 13ms, 21ms and 23ms for IDSDDIP, IDDIP, ADIP and MMIP. The delay is calculated for every millisecond of time per packet. This decrease in delay is due to the use of ECC and ECDSA signature generation and verification performed initially and subsequently of a nodes IP address configuration.

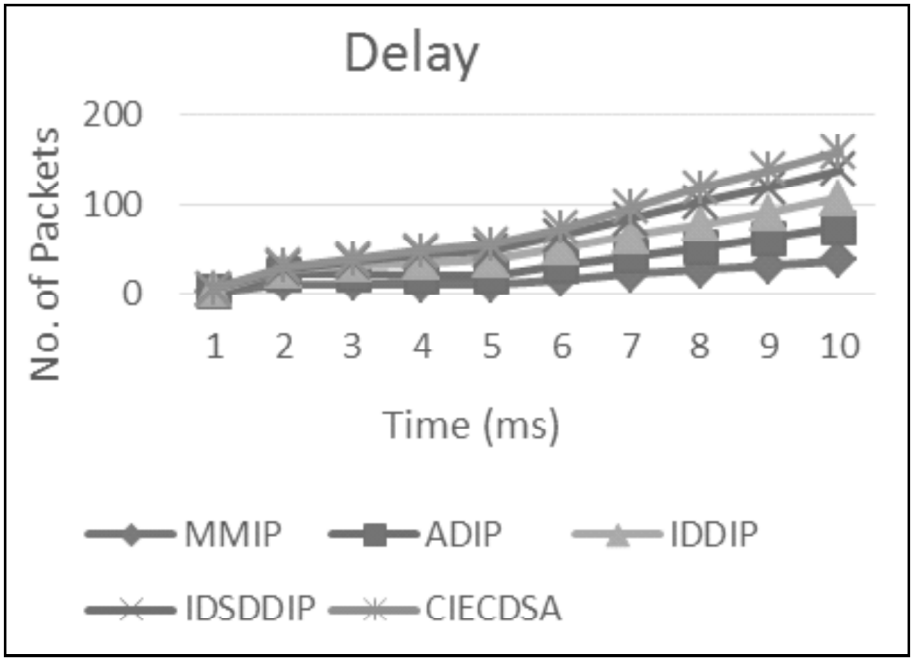


**Figure 4: End-End Delay**

(d) Latency: Latency is the interim period between the stimulation and response, or, from a more general perspective, as a period postponed between the reason and the impact of any physical change in the framework being watched. Figure. 5 show that the CIECDSA exhibits a low addressing latency of 0.175ms. The differences in values are 0.04ms, 0.08ms, 0.13ms and 0.15ms compared to IDSDDIP, IDDIP, ADIP and MMIP respectively. The ECDSA algorithm introduced in the address generation method reduces the complexity of O (2t+p+c), O (2t+p), O (2t+m) and O (2t) of IDSDDIP, IDDIP, ADIP and MMIP respectively. Therefore, the latency for CIECDSA is reduced as O (t).

(e) Communication Overhead: Communication overhead is those bits of data that must be sent to convey information. For example, the source of information, where it is being sent to, how it is to be routed, timestamps, or any other information that is not actually the “payload” represents the actual content to be communicated. Form the Figure. 6 below, initially both CIECDSA and IDSDDIP exhibits the same level of bar, but then later with the increase in time and the number of packets the overhead becomes reduced. The difference is due to the use of ECDSA signature verification and generation in X.509 certificate which reduces the overhead produced. The difference in values are 2.5ms, 3.5ms, 5.5ms and 8.5ms compared to IDSDDIP, IDDIP, ADIP and MMIP respectively The

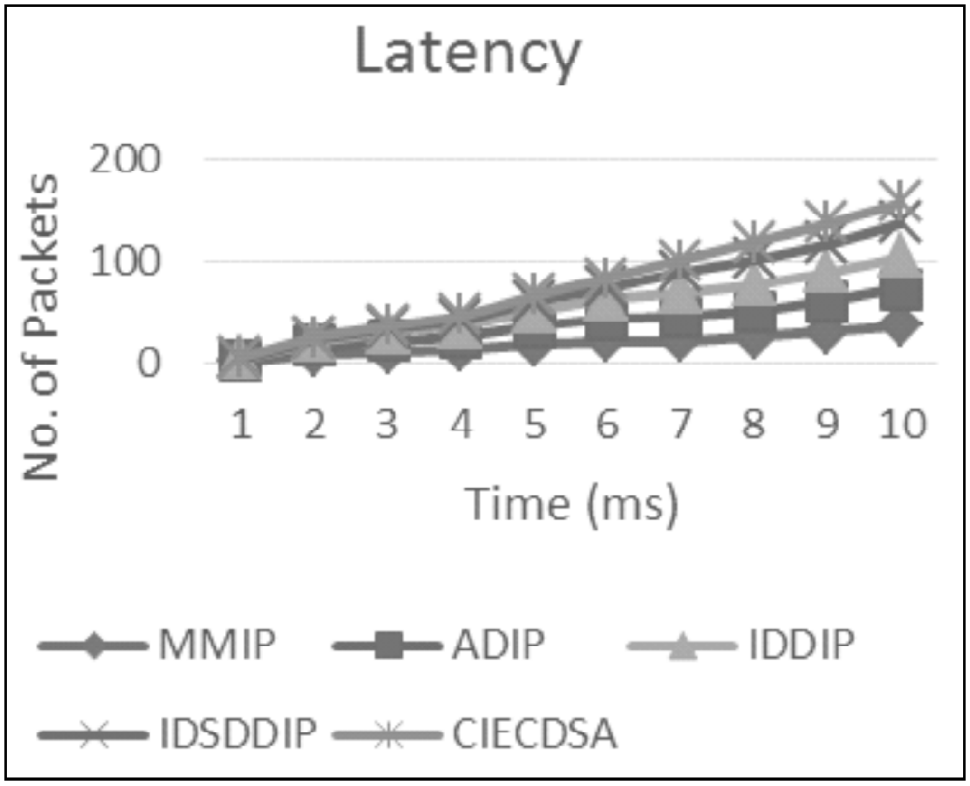


**Figure 5: Latency**

overhead reduces to O (n-1)/2 for CIECDSA, but for the existing schemes such IDSDDIP, IDDIP, ADIP and MMIP the complexities are O (n/2).Hence, the IP address configured is much more faster with higher security and robustness compared to the existing schemes.

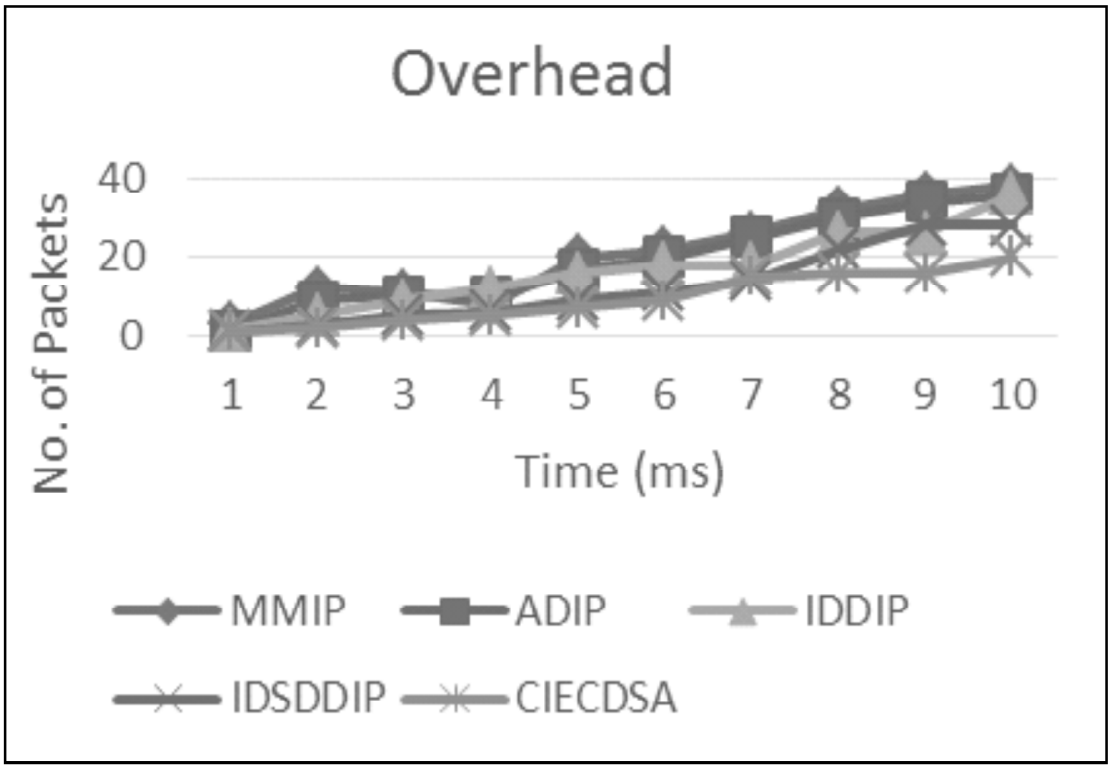


**Figure 6: Communication Overhead**

## 5. CONCLUSION

In this research work, an attempt has been made to propose an addressing mechanism in which Elliptic Curve Cryptography is implemented for MANETS with the help of signature verification and generation using Elliptic Curve Digital Signature Algorithm. In the algorithm every node processes ECDSA signature generation and verification which is embedded in the certificate. The percentage of improvement in throughput (increase in 3%, 10%, 13% and 16%), packet delivery ratio (increase in 16%, 24%, 26% and 28%), delay (decrease in 5ms, 13ms, 21ms and 23ms), latency (decrease in 0.04ms, 0.08ms, 0.13ms and 0.15ms) and communication overhead (decrease in 2.5ms, 3.5ms, 5.5ms and 8.5ms) of the proposed scheme, shows a remarkable improvement in comparison with the existing schemes such as the IDDSDIP, IDDIP, ADIP and MMIP respectively. Further, when compared to the existing IDDIP & IDDSDIP scheme it is more robust and more secure due to the use of X.509 certificate integrated in the algorithm for Manet IP addressing scheme.

## REFERENCES

[1] Droms R: Dynamic Host Configuration Protocol, RFC 2131, March 1997.

[2] Hemamalini. V, Dr. Zayaraz G 2013 A Survey on IP Configuration of Mobile Ad Hoc Networks with and without DAD Mechanism. *International Journal of Scientific and Research Publications* Volume 3, Issue 8, ISSN, 2250-3153.

[3] Xiaowen Chu, Jiangchuan, Liu Yi Sun 2009 Address Allocation Mechanisms for Mobile Ad Hoc Networks. *Guide to Wireless Ad Hoc Networks, Computer Communications and Networks*, S. Misra et al. (eds.), DOI 10.1007/978-1-84800-328-6_14, _ Springer-Verlag London Limited.

[4] Droms R: Dynamic Host Configuration Protocol, *RFC 2131*, March 1997.

[5] Y. Sun, E.M Belding-Royer, 2003 Dynamic address configuration in Mobile Ad Hoc Networks, *UCSB Tech. Rep*, pp. 2003–2011.

[6] Majid Taghiloo, Mehdi Dehghan, Jamshid Taghiloo, Maria Fazio 2008 New approach for address auto-configuration in manet based on virtual address space mapping (vasm). *International Conference on Information and Communication Technologies: from Theory to Applications (IEEE ICTTA*), Damascus, Syria, 7–11.

[7] Tajamolian M, Taghiloo M, Tajamolian 2009 M Lightweight secure ip address auto-configuration based on vasm. *International Conference on Advanced Information Networking and Applications Workshops, Waina'09*. pp. 176–180.

[8] Nesargi S, Prakash R 2002 Manetconf: Configuration of hosts in a Mobile Ad Hoc Network, *Proceedings of IEEE INFOCOM* p.p. 1059–1068.

[9] Y. Hsu, C. Tseng 2005 Prime dhcp: A prime numbering address allocation mechanism for manets. *IEEE Communicatons.* Vol. 9, No. 8, pages 712–714.

[10] Fazio M, Villari M, Puliafito A 2006 Aipac: Automatic ip address configuration in Mobile Ad Hoc Networks. *Performance Evaluation of Wireless Networks and Communications Computer Communications.* 29 (8): 1189–1200.

[11] Cavalli A, Orset J 2004 Secure hosts auto configuration in Mobile Ad Hoc Networks. *Data Communication and Topology Control in Ad Hoc Networks Ad Hoc Networks*. 3 (5): 656–667.

[12] Chu X, Sun Y, Xu K, Sakander Z, Liu J 2008 Quadratic residue based address allocation for Mobile Ad Hoc Networks. ICC '08. IEEE International Conference on Communications. Pages 2343 – 2347.

[13] Wang P, Reeves D S, Ning P, 2005 Secure address auto-configuration for Mobile Ad Hoc Networks. *Proceedings of 2nd Annual International Conference on Mobile and Ubiquitous Systems*: Networking and services, pp. 519-521.

[14] Uttam Ghosh, Raja Datta 2009 A new dynamic ip configuration scheme with mac address mapping for Mobile Ad Hoc Networks Mmip. *Proceedings Fifteenth National Conference on Communications* 4225-429.

[15] Uttam Ghosh, Raja Datta 2009 An improved authenticated dynamic IP configuration scheme for Mobile Ad Hoc Networks Adip. *Int. J. Ultra Wideband Commun. Syst*. 1 (2) 102–117.

[16] Uttam Ghosh, Raja Datta 2011 A secure dynamic IP configuration scheme for mobile ad hoc networks. *journal homepage: www.elsevier.com/locate/adhoc*, Volume 9, 1327-1342.

[17] Uttam Ghosh, Raja Datta 2012 An ID based secure distributed dynamic IP configuration scheme for mobile ad hoc networks. *ICDCN'12 Proceedings of the 13th international conference on Distributed Computing and Networking LNCS 7129* © Springer-Verlag Berlin, Heidelberg 295-308.

[18] Vijayalakshmi V, Palanivelu T G 2007 Secure Antnet Routing Algorithm for Scalable Adhoc Networks Using Elliptic Curve Cryptography. *Journal of Computer Science* 3 (12): 939-943 ISSN 1549-3636 © Science Publication.

[19] Kilian Weniger 2003 Passive duplicate address detection in Mobile Ad Hoc Networks. *WCNC, (Florence, Italy).*

[20] Padmavathi G, Lavanya B 2012 Comparison of RSA-Threshold Cryptography and ECC-Threshold Cryptography for Small Mobile Adhoc Networks. *Int. J. Advanced Networking and Applications* Volume: 03, Issue: 04, 1245-1252.

[21] Perkins C E, Malinen J T, Wakikawa R, Belding-Royer E M, Sun Y 2001 Ad hoc address auto configuration, *IETF Internet Draft, vol. draft-ietfmanetautoconf-01.txt*.