International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-2, Issue-1,January 2016
ISSN: 2395-3470
www.ijseas.com

OVERHEAD MINIMIZATION IN MANET USING IMPROVED ELLIPTICAL SECURITY ALGORITHM

M.CHARLES AROCKIARAJ[1], Dr.P.MAYILVAHANAN[2]
[1] Research Scholar, Vels University, Chennai. 600117,INDIA.
[2] HOD,DEPT.OF M,C,A, Vels University, Chennai. 600117,INDIA.

Abstract

MANET is an ad hoc network topology where the locations are self configured continuously without wires. The methodologies of MANETs are mobile and they have the ability to move independently in any direction. This configuration of MANET has routable networking environment as each of its devices are connected mainly to properly route the traffic. The main problem of using MANET connections is based on security. MANET does not have any safe security policy, so there is a possibility for lead active attackers to easily exploit or disable mobile network topologies. To discover the misbehaving attackers as well as to predict its effects, a new hybrid based algorithm named ECKCDSA with SHA 512 hash function is proposed in this paper. By using this algorithm the massive threats are detected with reduced computational overhead. Furthermore security parameters like packet delivery ratio, authorization and mutual authentication are gradually improved based on this new hybrid approach.

Keywords: MANET (Mobile Ad hoc NETwork), multi hop network, ECKCDSA (Elliptic curve Korean Certificate Based Digital Signature Algorithm), SHA (Secure Hash Algorithm).

1. INTRODUCTION

MANET is a growing technology, which enables users to commune without any substantial infrastructure in their geographical location. MANET is formed by the collection of transferable wireless devices. MANETs exhibits various security goals they are privacy, authentication, non-repudiation and integrity [1]. These types of goals can be achieved by maintaining a secured channel connection between the receiver and the sender. While the shortest path to transfer the information form one person to another mainly based on cost function and this directly determines the optimal route of the system [2]. The set of MANET applications are generally constrained by power resources mainly established on highly dynamic networks, mobile networks, and static networks. Several types of MANETs include SPAN (Smart Phone Ad Hoc networks), VANET (Vehicular Ad Hoc Network), IMANET (Internet based Mobile Ad Hoc Network) and Tactical/military MANETs.

Because of the vibrant nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET [3]. Based on the measures different protocols were enabled to carry out the systematic approach they are network throughput, the overhead introduced by the routing protocol, packet drop rate, end-to-end packet delays, ability to scale, etc. MANETs exhibit various challenges based on its issues in efficiency and performance namely packet loss due to errors in transmission, frequent network partitions, limited range of wireless transmissions, the time varying nature, characteristics of the wireless systems and route alterations due to mobility [4].

The application program of this wireless network topology is restricted due to mobile and ad hoc characteristics. The use of firewall in MANETs is prevented by using lack of centralized operation. Like wired networks, the wireless MANETs are faces many security threads. Some of the MANET attacks are denial of service, spoofing, routing procedure, passive eavesdropping, and many others [5].

A wormhole attack is a kind of attack that classically occurs with two or more venomous nodes in which the first malignant node eavesdrop or listen in packets at one location and then send them by passageway to second malicious node in an additional area. In the mobile ad hoc networks the data transfer will take place from node to node within the range of radio waves [6]. Transmitting the packet of data between these attackers can be done by using straight tunnel in wireless/wired connection. In the lack of safety mechanisms, the existing routing protocols may not be proficient to find a legal path to promote their data ensuing in isolation of a set or single data of mobile nodes. Hence, an efficient and reliable defense mechanism is required to detect the hollows in an ad hoc network.

The main purpose of this paper is to propose successful security algorithm which improves the security related issues based on invader nodes and packet drop rate. The planned work is designed to have a protected key association to predict the attacker's incidence in order to recognize the misbehavior nodes with various possibility in parameters based on evaluation. The study compares various other hybrid algorithms like ECC, HAPMON with the ECKCDSA SHA 512 to relate its performance analysis. Based on certain parameters like key generation, packet drop ratio, computational and communication overhead the proposed algorithm tend to produce higher performance based on the results obtained.

The rest of the paper is organized as: section II deals with literature survey of previous methods with demerits and its overcoming methodologies, Section III gives the elaborated explanation of proposed hybrid authentication algorithm and its methodologies with its advantages by comparing with previous methods, section IV evaluates the results and discussions of the paper and section V discusses the conclusion of the paper.

II. LITERATURE SURVEY

A great deal of studies has been carried out infrastructure based wireless network with MANET networks. However, M Janardhana Raju et al., reviewed the basic necessities of communication networks which paved the way for the growth of wireless communications all over the world [7]. The Mobile Ad hoc networks are wireless networks therefore there is a possibility of formation of attacks which includes Denial of Service leading to failures in system resources like memory, power and Bandwidth. Bhavana Sharma and vandhana Madaan [8] viewed MANET as a prominent technique in wireless networks with great care by different groups. A mobile Ad hoc network is a collection of wireless mobile nodes which are inclined to form a system without any fixed infrastructure having self configuring and mobile nodes. Nowadays securities in MANETs play a major important role in mobile Ad hoc networks based on its basic parameters like packet drop rate and end to end delivery rate.

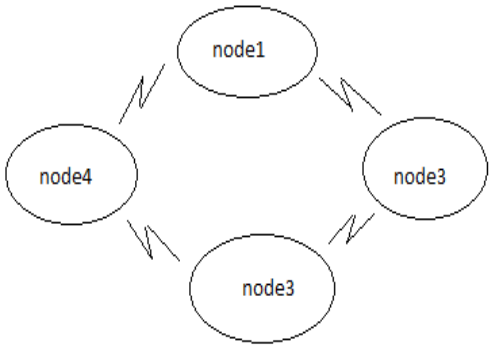


Fig 1: Ad hoc wireless network

In the above figure, 4 nodes are connected in wireless network topology. Each device in the node independently moves from one node to another node without limitations in all direction and it configures its links to other private devices. Elliptical curve based cryptography provides a hopeful solution to increase the safety measures of MANETs than other existing popular algorithms such as RSA. The ECC-

TC using GNU Multi precision Library (GMP) confronts the security issues for the employment in MANETs.

Michael Braun and Anton Kargl., [9] discussed the major security goal for signature schemes to prevent the adversary from producing new valid signatures from the legitimate signer. Major elliptical curve signature schemes such as ECDSA, ECKDSA or ECGDSA based on elliptical curve discrete logarithms on the security of the used hash function were proposed in this paper. Santhi Sri [10] proposed a new intrusion detection system with ECC algorithm particularly designed for MANETs. Edna Elizabeth et al., [11] proposed various security variation schemes namely digital signature algorithm and elliptic curve cryptography. Numerous points which are generated based on elliptic curve of prime field are chosen at random as a secret key. To transmit the secret key to all the users the public key generation forms a public key generation. By using the RSA algorithm the secret key which is to shared is encrypted. Then finally the concatenated chain along with signature pair is sent through the protected channel.

Greeshma Sarath et al., [12] studied various security aspects of ECDSA and proposed certain variants based on security levels and execution time. The ECDSA algorithm mainly consists of 3 phase's namely key generation, signature generation and signature verification. ECKDSA is a Korean Certificate based Digital Signature Algorithm by which the public key is supported by means of a certificate issued by some trusted authority. Sathya Priya et al., [13] reviewed the various reasons for the attacks on MANET as unfixed topology, unreliability, lack of centralized control and limited battery power. The misbehavior nodes in the network are detected by using a scheme called Enhanced Adaptive Acknowledgement (EAACK). This can detect the misbehaving nodes in the network but cannot choose upon which the misbehaving node is linked with. This type of misbehaving node is called as black hole attack. In this study a path tracing algorithm is proposed which determines the certain parameters namely packet delivery ratio, end to end delay, and routing overhead.

Ramya et al., [14] evaluated an intrusion detection system called Enhanced Adaptive ACKnowledgement (EAACK) particularly for mobile networks. The EAACK was designed based on RSA and DSA. The strength of the security in mobile ADHOC networks are designed by using an advanced innovatory approach called Hybrid Security protocol which increases confidentiality, authentication and integrity. This algorithm mainly consists of Dual RSA algorithm, cryptography elliptical curve and message digest MD5. This new security procedure has been deliberated for better security using a mixture of both asymmetric and symmetric cryptographic proficiencies.

III. ***RESEARCH METHODOLOGY***

Secure and hybrid authentication protocol

In today's world, the use of Mobile networks plays an important role in tender related services. These tender related services include M-Learning, M-business where the data security play an important role with its expectation. Un-authentication is one of the major cause for this analysis. So in order to identify the authenticity in mobile networks cryptographic technique is used. The hybrid scheme of the key authentication organization is implemented using cross layer intrusion detection systems. The misbehavior attacks can be identified using fuzzy logic based methodology. The hybrid procedure is used to utilize the packet loss because of limited power function or malfunction. Moreover, the detection of the misbehaving nodes and the anticipation of its symptoms are calculated by using Fuzzy logic function. The proposed hybrid scheme aims to watch over the misconducting nodes, to predict the nodal activity, to identify the packet drop

ratio by estimating certain parameters such as packets dropping, possibilities of affected packets and possibilities attacker ratio due to misbehavior characteristics in the performance of the nodes.

The proposed secure hybrid authentication protocol consists of organizer nodes, servers, and typical movable nodes. For the Trusted Authority Authentication, one organizer node is selected. The proposed protocol design in this paper is made up of Self Trusted key management method of the MANET. It integrates the common nodes which are chosen as the administer node [15]. The administer node always stands as central nodes for transferring messages from typical changeable nodes to the servers. Various authentication protocols for security related issues are,

i. RSA (Rivest Shamir Adelman)
ii. ECC(Elliptical Curve Cryptography)
iii. Modified ECC

The detailed explanation of the above mentioned protocols are given below with detailed explanation. Finally, the modified ECC tend to be exhibit high reliability and capability when compared with RSA and ECC.

i. RSA

RSA is a special type of algorithm which uses public key and private key for encrypting and decrypting the methodological topology. This RSA algorithm is a highly secure public key encryption algorithm. In the public key technology of crypto systems, RSA exhibit public key encryption so that everyone can find it. Rather private key encryption should be mainly kept in hidden [16]. The main purpose of the public key is to encrypt the message while the private key is used to decrypt the message. By using this methodology, it is difficult to find what private key is used for public key. The algorithmic principle of the RSA is briefly explained as follows: Initially the public key and the private key models are randomly generated. The next step is to generate the keys in the most unpredictable and random manner. Then the sharing of resources to all parties is carried out using private key. Using RSA-TC algorithm random numbers are generated with N-computation. The generation of random numbers is carried out with basic renowned steps of methodological functions. There are two parties p and q, each picks secret numbers i as pi and qi. All the parties determine the sums by determining the divisibility of the prime number between 0 to some bound. The values of p and q remain unknown to all the parties as required based on the analysis.

$$p = \sum_{i=1}^{n} pi$$
$$q = \sum_{i=1}^{n} qi \qquad (1)$$

The distributed computation of N is computed when all the parties come together to examine N as unknown value to every person [17]. Each party pi knows the tuple and keeps it secret from other parties, by making the following four conditions satisfied:

$$N=\left(\sum_{i=1}^{n} pi\right)\left(q = \sum_{i=1}^{n} qi\right) \qquad (2)$$

Generation of Private Key

Holding to computed N and public key encryption component e, each party now computes its own private additive share di, of the decryption key d as,

$$d = \sum_{i=1}^{n} di + x * de = 1(\text{mod } N) \qquad (3)$$

The threshold concept is applied by means of splitting‘d’. The key d should be splitted by means of n shares of secret t. Based on this approach t+1 cryptographic operation were successfully performed.

Encryption

The encryption procedure is carried out by using shared RSA scheme accepting N= pq. The

public components are moduli N and the encryption exponent e is co-prime to N.

$$C = mi^{ei} \bmod N \quad (4)$$

Decryption

For 'n' parties the prime factors N remain unknown to every person. Each party has a set of values unknown to each other. For example if the value of pi is generated the result of that value will be kept in secret with other two parties' qi and di . So in order to set with the above basic steps, certain algorithmic procedures should be followed as given below parameters,

$$p = p1 + p2 + \ldots\ldots\ldots + pn = \sum_{i=1}^{n} pi$$
$$q = q1 + q2 + \ldots\ldots\ldots + qn = \sum_{i=1}^{n} qi$$
$$d = d1 + d2 + \ldots\ldots\ldots + dn = \sum_{i=1}^{n} di \quad (5)$$

The multiplicative notation of decryption key and encryption component is determined as,

$$ed = 1(\bmod \phi(N)) \quad (6)$$

The final result is computed as,

$$mi = c^{di} \bmod N \quad (7)$$

The RSA algorithm exhibits certain drawbacks based on the analysis and systematic functions they are- the use of prime numbers sometimes may be very small and close to the factorization of N. This may cause the resultant outcome to get restored from the higher capability of resources to lower one. Unobservable e^{th} power may cause the systematic approach to get easily retrieve the plain text [18]. There are many attacks using this RSA algorithm they are Hastad's attack**,** Coppersmith's attack etc. In order to overcome the attacks and the drawbacks, ECC cryptosystem is exhibited.

ii. ECC

ECC is one of the fastest computational methodologies with smaller key sizes, lower power consumption topology, lower bandwidth etc [19]. The conventional crypto systems function directly on long entries where the point which belongs to the elliptical orbit is defined over finite field. The equation of elliptical curve is given as,

$$y^2 = x^3 + ax + b \quad (8)$$

The key generation is the main part to be undertaken when holding with encryption and decryption methodologies. In the encryption process a selected number d with a range of n is selected. The representation is carried out as,

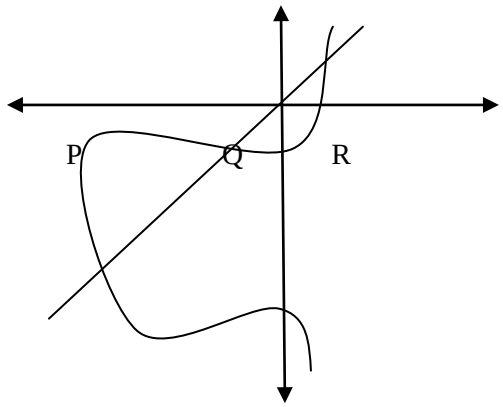


Fig 2 Representation of ECC

$$Q = d * p \quad (9)$$

Q is the public key, d is the selected random number private key with p as the curve point. Let m be the message sent with the implementation details. The selected k is represented within k from 1 to (n-1). Two cipher texts are generated based on the analysis they are,

$$C_1 = k * p \quad (10)$$
$$C_2 = M + k * Q \quad (11)$$

After encrypting the message the information should be sent to the original form which is represented as,

$$M = C_2 - d * C_1 \qquad (12)$$

Then the final message M is obtained by cancelling *K*P*Q*.

The main drive of ECC relies on the difficulty in solving various equations which deals with ECDLP (Elliptical Curve Discrete Logarithmic problem). The main cryptographic approach of ECC is scalar point multiplication with $Q=k\ P$. ECDLP states that for given P and Q it hard to find *K* in ECC. By using the combination of point doublings and point additions, the scalar point multiplications are performed. By using ECDLP with the given P and Q, it is hard to find *k* [20]. The integer k acts as a private key while the multiplication of Q act as a corresponding public key. The ECC crypto operations are characterized by using ANSI, INTF, IEEE and NIST. By using this analysis, the security attacks of the system can easily be evaluated. The main advantage of ECC includes smaller key size, highly secure and no certificate is needed to bind the names to public keys. Some of the drawbacks using ECC include increase in network overhead, and elimination in necessities of pre distribution keys.

iii. Modified ECC with ECKCDSA based on SHA 512 hash function:

The main aim of going to ECKDSA with SHA 512 has function is based on its advantages in security related issues. Some of the advantages of using modified ECC include strong security, higher speed and smaller key size [21].

Parameter analysis of ECKDSA

The main domain parameter of elliptical field parameter includes finite field and ones that is added with elliptical curve finite field [22]. For ECKDSA the following parameter are considered they are monic irreducible polynomial k, prime and positive integers r and s defining a field, Coefficients (x_1,y_1) defining the elliptical curve e over G K(p), private signature key x selected at random over Z_q, prime q dividing the order of elliptical curve with total number of points as e, hashed certification data h_{cert}, point G= Base element order, associated public verification key D_A with message m is generated with the pair of integers.

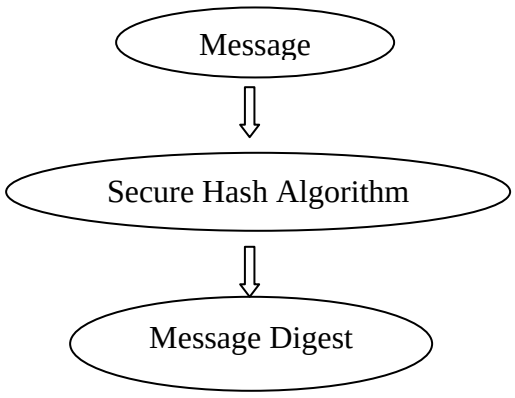
Signature Algorithm

The two basic group of analysis are carried out using this signature algorithm they are signature generation and signature verification.

Signature generation

To generate a signature on signing and verifying process on message m, the signer should take into account of the following parameters [23]. Two parts with first part r and second part s of the algorithm should be taken for consideration. The basic steps of the signature generation approach is given below,

1. Select random value $k \in (1, n-1)$
2. Compute $KG=(x_1 , y_1)$
3. The calculate $r = Hash(x_1)\ mod\ n$. If $r=0$, continue to step 1.
4. Compute $e = Hash(h_{cert} \| m)$
5. Compute the integer $w = r \oplus e \pmod n$
6. Computes $e = r \oplus h(W)$
7. Compute the second part *s* of the signature $s= d_A(k-w)$. If $s=0$, then go to step 1.
8. The signature m is the pair of (r,s).



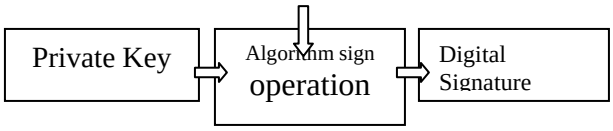


Fig 3 Signature Generation

Signature Verification

To verify the signature $\{ m \| s \| r \}$ the verifier should be taken into account with the following steps [24].

1. Compute $e = Hash(h_{cert} \| m)$
2. Compute the integer $w = r \oplus e(\mathrm{mod}\, n)$
3. Compute $X=(x_1,y_1) = wG+sD_A$
4. If $X=0$, reject the signature. Otherwise compute $v = Hash(x_1)$ mod n
5. Finally check and accept the signature only if $r = v$.

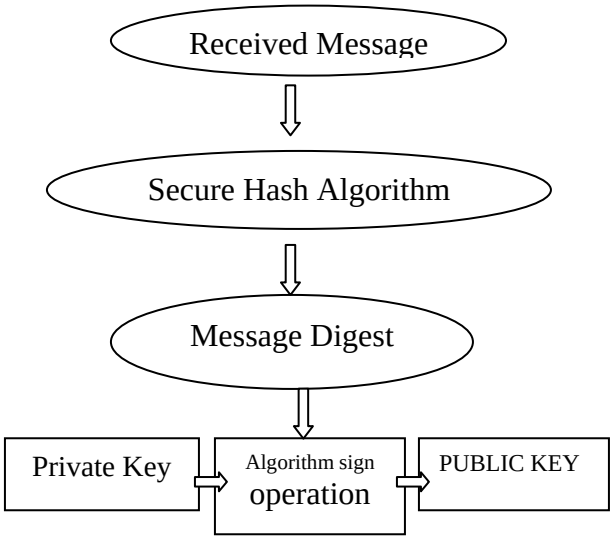


Fig 4 Signature verification

The main advantages of using ECKCDSA WITH SHA 512 hash function are reduced computation overhead and communication overhead, reduced DOS attacks while transferring the data within the network and increase in packet delivery ratio.

IV RESULTS AND DISCUSSION

The performance of the RSA, ECC and modified ECC using ECKDSA SHA-512 algorithm is compared with various analysis parameters such as key generation, packet delivery ratio, communication overhead and computational overhead. For ad Hoc networks, ECKDSA SHA-512 offers complete unlikability, content unobservability and privacy protection. Based on node compromise analysis, this ECKDSA provides strong security protection and is also more defiant against attacks. The packet delivery ratio is defined as the ratio of number of data packets actually received to the total number of packets sent. The communication overhead is related to losses in the resources which deal with the transfer of data/information from the source to the destination. Throughput is defined as the ratio of time difference between sent packets and received packets.

Throughput= (Received packets /Sent packets)* 100%

Table 1 Comparison Table

PARAMETERS	RSA [17]	ECC [17]	MODIFIED ECC [19]
Key size generation (in bits)	1024	163	160
Time taken for key Generation	0.16	0.08	0.25
Packet delivery ratio	0.9	0.87	0.93
Encryption throughput	993.80 KBps	61.93 KBps	84.36 KBps
Decryption throughput	996.79 KBps	33.11 KBps	46.72 KBps

To increase the future research direction of this paper certain investigations to reduce the network overhead and the concept of adopting key exchange mechanism should be taken into account.

V CONCLUSION

In this research work, the Hybrid and secure authentication protocol methodology is proposed based on ECKCDSA SHA512 hash function which improves the detection of the misbehavior nodes with the attacker by enhancing the system security. This methodology deals with the expansion of the network protocol, which is more appropriate for Network Trust Organization Server. In this approach, the authentication protocols – RSA, ECC and modified ECC on key management which has high security encryption was discussed. Hence, this authentication protocol has more security to attacks on data transfer, highly reliable to forecast the misbehavior nodes with the following parameters by considering the performance of the proposed system based on computation storage overhead, predicting the attacker precision, and prediction of packet loss. Thus the protocols have been analyzed under the strongest attack model which undergoes the step process by determining the network security in the DOS assault model. Finally, the routine parameters are engaged by determining the prediction of accuracy and its misbehavior nodes, as well as verification protocol of proposed system under different perspectives as with signature generation and signature verification.

References

[1] Ankur O. Bang, Prabhakar L. Ramteke (2013) MANET: History, Challenges and Applications IJAIEM Volume 2, Issue 9 .pp.249-251.

[2] Kristin Lauter, (2004) “The Advantages of Elliptic Curve Cryptography for Wireless Security” IEEE vol no 20 .pp.62-67.

[3] Vijayakumar and Tamizharasan (2013) Enhancing the Secure Data Transmission for Routing Attacks in MANET IJARCSSE vol 3 no 11.pp.404-411.

[4] Rajesh Yadav and Dr. Srinivasa Rao (2015) A Survey of various routing protocols in MANETs IJCSIT vol 6 no 5.pp. 4587-4592

[5] Priyanka Goyal et al (2010) A Literature Review of Security Attack in Mobile Ad-hoc Networks IJCA vol 9 no 12.pp.11-15.

[6] Dinakar and Dr. J. Shanthini (2014) A Study on Various Features of Multicast Routing Protocols in Mobile Ad hoc Networks IJARCSSE vol 4 no 7.pp.612-616.

[7] Raju et al., (2013) A Novel Elliptic Curve Cryptography Based Aodv For Mobile Ad-Hoc Networks For Enhanced Security JATIT Vol 58 No 3.pp.349-357.

[8] Bhavna Sharma and vandhana Madaan (2015) Enhancing Security of MANETs by Implementing Elliptical Curve based threshold Cryptography IJECS Vol 4 no 7 .pp. 13346-13350.

[9] Michael Braun and Anton Kargl (2007) A Note on Signature Standards Siemens corporate Technology IEEE .pp. 1-7.

[10] Santhi Sri et al (2014) Minimizing Network Overhead in MANET Using Elliptic Curve Cryptography IJRCCT Vol 3 no 8 .pp.901-904.

[11] Edna Elizabeth et al (2013) Enhanced Security Key Management Scheme for Manets Wseas Transactions On Communications vol.13 .pp. 15-25.

[12] Greeshma Sarath et al (2014) “A Survey on Elliptic Curve Digital Signature Algorithm and Its Variants” CSCP .pp.121-136.

[13] Sathya Priya And Krishnakumari (2014) Detection Of Misbehavior Nodes In MANET Using Path Tracing Algorithm IJRASET Vol 1 No 1.pp.11-16.

[14] Ramya et al (2014) Hybrid Cryptography Algorithms for Enhanced Adaptive Acknowledgment Secure in MANET IOSR-JCE vol.16 no 1.pp.32-36.

[15] Jayrajsinh Jadeja A Review on Detection of Wormhole Attack in Mobile Ad-hoc Networks ISSN: 2321-9939 (2003) A Review on Detection of Wormhole Attack in Mobile Ad-hoc Networks vol 3 .pp. 153-157.

[16] Praveen kumar et al (2014) Providing a New EAACK to Secure Data in MANET IJREAT vol 2 no 2 .pp.1-5.

[17] Rashmi K. Mahajan and Prof. S. M. Patil Eaack (2014) Secure IDS For Manet By Using Cryptographic ECDSA Algorithm vol 2 no 12 .pp.97-102.

[18] Pranjali D.Nikam and vanitha Raut (2015) Enhancement to EAACK for improved MANET security vol 3 no 5 .pp.324-329.

[19] KCDSA Task force Team (1998) The Korean certificate Based Digital Signature Algorithm ASIACRYPT .pp.1-14

[20] Hung-Yu Chien (2003) A hybrid authentication protocol for large mobile network ELSEVIER vol 67 no 10.pp.123-130.

[21] G.Padmavathi and B. Lavanya (2012) Comparison of RSA-Threshold Cryptography and ECC-Threshold Cryptography for Small Mobile Adhoc Networks IJANA vol 3 no 4.pp. 1245-1252.

[22] Lijun Liao and Mark Manulis (2007) Tree-based group key agreement framework for mobile ad-hoc networks ELSEVIER vol 23 .pp.787-803.

[23] Nicholas Jansma and Brandon Arrendondo (2004) “Performance Comparison of Elliptic Curve and RSA Digital Signatures”

[24] ANR Project ECLIPSES (2012) Elliptic Curve Leakage-Immune Processing for Secure Embedded Systems.pp.1-43.