Enhanced Security Key Management Scheme for MANETS

EDNA ELIZABETH.N, SUBASREE.S, and S.RADHA
Electronics and Communication Engineering Department
Sri Sivasubramaniya Nadar College of Engineering
Kalavakkam, Chennai-603110
INDIA
ednaelizabethn@ssn.edu.in

Abstract: - (MANET) Mobile Ad hoc Network is a collection of wireless infrastructure less network. The topology of the network changes continuously. Due to the dynamic structure of MANETs, they are prone to various types of attacks. The traditional security solutions for MANETs are inadequate, hence security should be maintained at all the levels. To enhance security various schemes have been proposed. In this article the security is provided by two schemes namely the elliptic curve cryptography and the digital signature algorithm. Various points are generated from the elliptic curve of prime field and a point is chosen at random as a secret key. The public key generation centre forms the secured channel for transmitting the secret key to all the users in the MANET. Now the secret key to be shared is encrypted using the RSA algorithm. The keys before sending and receiving must be signed by the sender and verified by the receiver thereby authenticating each other. The encrypted secret key is concatenated along with the signature pair key and is sent through the secured channel. Thus the security is enhanced at various levels which prevent strong malicious attacks.

Key-Words: - HADS (Hash Asymmetric Digital Signature), ECC (Elliptic Curve Cryptography), DSA (Digital Signature Algorithm), BHA (black hole Attack).

1 Introduction

MANET (Mobile Ad hoc Network) is a wireless infra-structure less network. It is dynamic in structure which changes its topology frequently according to its needs. Thus it is prone to various types of attacks. The attacks in MANETS are due to their open medium, absence of fixed or central structure, dynamically changing topology, constrained capability etc. Security goals such as integrity, authenticity, non-repudiation, privacy etc., have to be considered in MANETS [1]. This can be achieved only by using a secured channel between the sender and the receiver. Hence forward secrecy and backward secrecy has to be maintained. Forward secrecy is nothing but when the member leaves the group, the member should not hear further conversations in the group. Similarly backward secrecy refers to that when a new member joins the group, the member should not be able to access the previous conversations in that group [1]. Many encryption and key sharing techniques are implemented in MANETs. The levels in nodes and the secured channel for key exchange are formed by using ECC, IBE (Identity Based Encryption) and Shamir's (t,n) threshold cryptography [2]. In this article, to enhance security for routing, ECC along with hashing function, DSA, and RSA are implemented instead of using IBE as mentioned in [2]. The paper [18] has implemented NRMT (Neighborhood Route Monitoring Table) algorithm that does not compare with any other secured protocol. Our results are compared with the NRMT protocol [18] in the presence of black hole attack. Our results show better performance in terms of packet delivery ratio, end to end delay and overhead.

2 Related Works

Wan An Xiong, et, al [2] [2011] discusses about Elliptic curve Cryptography, Identity based Cryptography and Shamirs (t,n) threshold cryptograpy. Nonlinear pair computation is applied to realise secure key management and communication. Shamirs (t,n) threshold cryptography is used to build three level security in ad hoc network. This scheme can be applied to dynamic toplogy and different sizes of ad hoc network. This scheme does not require any

certificate management. It can get a high security with few traffic and computation. It does not give any simulation proofs. Also the three level topology can be replaced by SRT [17] that uses simple topology with reduced overhead.

Maria Celestin Vigila S, et, al [3] [2009] discusses the implementation of text based Elliptic Curve Cryptosystem. Each character in the message is represented by its ASCII value. Each of these ASCII value is transformed into an affine point on the EC, by using a starting point called Pm. Transformation of the plaintext ASCII value by using an affine point is one of the contributions of this work. The purpose of this transformation is two folds. Firstly a single digit ASCII integer of the character is converted into a set of co-ordinates to fit the EC. Secondly the transformation introduces non-linearity in the character thereby completely camouflaging its identity. This transformed character of the message is encrypted by the ECC technique. Decryption of ECC encrypted message is itself quite a formidable task, unless we have knowledge about the private key 'nB' ,the secret integer 'k' and the affine point Pm. These advantages are particularly beneficial in applications where bandwidths, processing capacity, power availability or storage are constrained. Such applications include chip cards, electronic commerce, web servers and cellular telephones. One of the applications that the ECC can be used for is encryption of large image files. The selection of the primes and the faster multiplication and doubling algorithms are the focus of research, the image encryption using ECC is completely a new domain and has tremendous scope of research.

Durgesh Wadbude, et al, [4] [2012] proposes an approach that uses improved security mechanisms to introduce in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and the Protocol Enforcement Mechanism. The performances of these two protocols (SAODV and ARAN) were tested in simulation and their communication costs were measured using the NS-2 simulator, which is suitable for the present purpose. The evaluation metrics used are overhead and end to end delay. In proposed scheme along with digital signature and hash chain ECC points are used for generation of secret key

Prakash Kuppuswamy, et al, [5] [2012] proposes method of Digital Signature Scheme based on the linear block cipher or Hill cipher. It is basically symmetric key algorithm. Digital Signatures can provide added assurances of the evidence to identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. But this method is a conventional method

Bin Sun et al, (2009) [6] analyses three layered key management architectures to Mobile Ad hoc networks (MANET) with three-layered virtual infrastructure. Two kinds of three layered key management architectures are introduced. The communication efficiency of them has been analysed. It also shows that the communication cost of the three-layered key management schemes is always smaller than that of the two layered ones. These two conditions can be used to optimize the MANET virtual infrastructure protocol. It also shows that the communication cost of the three-layered key management schemes is always smaller than that of the two-layered ones.

Fiat A et al, (1999) [7] proved the signature and identification scheme which enables the user to prove the identity and the authenticity of the message to other users without shared or public keys. This scheme is secure against any known or chosen message attack. It is very simple and secure and it is suited for microprocessor devices.

Menezes A et al, (1991) [8] analyses the reduction of the elliptic curve logarithm problem to the logarithm problem in the multiplicative group of an extension of the underlying finite field.

Haiyun Luo et al, (2004) [10] analyses ticket certification services through multiple node consensus and fully localized instantiation. It uses tickets to identify and grant network access to well-behaving nodes. In URSA, no single node monopolizes the access decision or is completely trusted. Instead, multiple nodes jointly monitor a local node and certify its ticket. Experimental and simulation results are analyzed for various parameters.

Jin-Hua Hong et al, (2009) [12] implements Elliptic Curve Cryptography on GF (2^{163}) using polynomial at the base. The encryption and decryption is implemented on the ECC chip, which needs fast operation and low hardware resources.

Gaga deep et al, (2012) [13] and Nishu Garg et al, (2009) [9] focuses the various types of attacks on various layers under protocol stack. Different types of attacker attempts different approaches to decrease the network performance, throughput. In this paper the principal focus is on routing and security issues associated with mobile ad hoc networks which are required in order to provide secure communication. On the basis of the nature of attack interaction, the attacks against MANET may

be classified into active and passive attacks. Attackers against a network can be classified into two groups: insider and outsider. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs.

Himadri Nath Sahaet al, (2011) [14] proposes a protocol for detecting flooding, black hole, gray hole and blackmail attacks and taking measures against the nodes committing them. This scheme is based on a concept of an underlying backbone network of administrator nodes that we assume to be trustworthy and honest throughout. These administrators have greater transmission and reception range than the general nodes in the MANET and have the power to take corrective actions on the basis of the reports sent by the other nodes. The association of these administrator nodes is dynamically increased to ensure better network coverage by upgrading certain general nodes to become administrators subject to certain constraints such as the transmission and reception range and the performance over a sufficiently large period of time.

Mamatha G.S, et al, (2010) [15] implements the identification and prevention of malicious nodes launching packet dropping and message tampering attacks, using a semantic security mechanism. This security scheme is highly impossible to break, thereby making it a highly secured approach. The evaluation results demonstrate that the approach effectively detects and prevents such nodes and links in networking sessions.

All the above schemes provides security for the network, but the proposed scheme enhances the security to a higher level by introducing ECC for key generation, RSA for encryption and decryption, and digital signature scheme with hash function for securely transferring the key to the users in the network with reasonable overhead.

3 Proposed Security and Key Management Scheme

This article uses EC points for choosing the secret key, and then Lagrange interpolation for sharing the secret key.

3.1 Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields [1]. Elliptic curves are always cubic. ECC is defined over the elliptic curve

$$y^2 \bmod p = \left(x^3 + ax + b\right) \bmod p \quad (1)$$

$$\text{Where } \left(4a^3 + 27b^3\right) \bmod p \neq 0$$

For two distinct points P= (x_p, y_p) and Q= (x_q, y_q) that are non-negatives of each other, the slope of the line *l* that joins them is given below [10]

$$\Delta = \frac{y_q - y_p}{x_q - x_p} \quad (2)$$

There is exactly one other point where *l* intersects the elliptic curve, and that is the negative of the sum of P and Q. After some algebraic manipulation the sum R=P+Q is given by,

$$x_r = \left(\frac{3x_p^2 + a}{2y_p}\right)^2 - 2x_p \quad (3)$$

$$\text{and } y_r = \left(\frac{3x_p^2 + a}{2y_p}\right)^2 \left(x_p - x_r\right) - y_p \quad (4)$$

The point can be able to be added itself by considering P+P=2P=R. When $y_p \neq 0$, the expressions are,

$$x_r = \Delta^2 - x_p - x_q \quad (5)$$

$$y_r = -y_p + \Delta\left(x_p - x_r\right) \quad (6)$$

A key exchange between users A and B can be accomplished as follows,

Step1: A selects an integer *nA* less than *n*. This is A's private key. A then generates a public key $P_A = nA*G$; the public key is a point Eqn (a, b).

Step2: B similarly selects a private key *nB* and computes a public key P_B.

It obtains the secret key $K=nA*P_B$. B generates the secret key $K=nB*P_A$

Similarly the encryption and decryption can be obtained by the following

An encryption/decryption system requires a point *G* and an elliptic group Eqn (a,b) as parameters. Each user A selects a private key *nA* and generates public key $P_A=nA*G$. To encrypt and send a message P_m to B, A chooses random positive integer *k* and produces the cipher text *Cm* consisting of the pair of points.

$$C_m = kG, P_m + kP_B \quad (7)$$

To decrypt the cipher text, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point.

$$p_m + kp_b - n_B(kG) = p_m + k(n_B G) - n_B(kG) = p_m \quad (8)$$

A has masked the message P_m by adding kP_B to it. No one except A knows the value of k, so even though P_B is a public key, nobody can remove the mask kP_B. However, A also includes a "clue", which is enough to remove the mask if one knows the private key nB. For an attacker to recover the message, the attacker would have to compute k given G and kG, which is assumed hard in elliptic curve cryptography [1].

3.1.1 Lagrange Interpolation Formula

The secret key is shared among the users by using the Lagrange interpolation formula [3]. It is the N^{th} degree polynomial approximation formula to the function $f(x)$ and the N^{th} degree polynomial approximation passing through (N+1) points. The coefficients of an unknown polynomial $f(x)$ of degree less than t, defined by points (x_i,y_i), $1 \le i \le t$, are given by the Lagrange interpolation formula

$$f(x) = \sum_{i-1}^{t} y_i \cdot \prod_{\substack{1 \le j \le t \\ j \ne i}} \frac{x - x_j}{x_i - x_j} \qquad (9)$$

Since $f(0)=a_0=S$, the shared secret may be expressed as:

$$s = \sum_{I=1}^{t} c_i . y_i, \text{ where } c_i = \prod_{1 \le j \le t} \frac{-x_j}{x_i - x_j} \qquad (10)$$

Each group member may compute S as a linear combination of t shares y_i. Since the c_i are non-secret constants. It means that for a fixed group of t, users may be pre-computed. So the secret key is shared among the users by computing the values of $f(0), f(1), f(2)$ etc..

An elliptic curve is chosen and various points are generated from the curve. A secret key is chosen and it is shared among the users by using the generated points of the elliptic curve. The secret key can be retrieved if there is no intruder between the users. The key shared among the users has to be encrypted while transmitting at the sender end and the receiver retrieves it using the Lagrange interpolation formula. Thus the secret key is shared among the users.

3.2 Secured Channel in MANET.

The key generated using ECC is now shared among the users through a secured channel. Hence for this purpose Hash algorithm, encryption and decryption using RSA and Digital signature scheme are used. This scheme is called HADS scheme that enhances security.

3.2.1 Hashing Algorithm

The **MD5** message-digest algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. An MD5 hash is typically expressed as a hexadecimal number, 32 digits long. MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512 [1].

The public key generation center forms the secured channel in the MANET.

P_{PKG} - Public key of the public key generation center.

S_{PKG} - Private Key of the public key generation center.

G - Generator from the elliptic curve.

$P_{PKG} = S_{PKG} \times G$

A-user or node A, B-user or node B

When a set of nodes are ready to form a MANET, they authenticate and communicate with each other with the help of public key and private key. Let us consider that node A wants to communicate with the node B.

The public key of node A can be calculated by the formula $Q_A=h_0(ID_A)$ where,

Q_A - public key of A
ID_A - identity of node A
h_0 - hash function

The private key if A can be calculated as
$S_A = S_{PKG} \times Q_A$
S_A -private key of A

The sender calculates the following, to send the secret key through the secured channel.

It randomly selects a point $\mathbf{x_q}$ from the elliptic curve and then selects a key from the elliptic curve as $\mathbf{k_q = (x_q, y_q)}$

K_q - secret key
(x_q, y_q) - Points on the elliptic curve

Then it calculates $\mathbf{r_b = m^{yq}}$. The key is concatenated with the r_b

m - Message or Secret key

r_b - is a variable for assigning the value of m.

The message m is concatenated with the value of r_b which is given by $(r_b||m)$.

3.2.2. Encryption and Decryption using RSA

The RSA scheme is a block cipher in which the plain text and cipher text are integers between 0-*n*-1 for some *n*. The steps for encryption and decryption are as follows [1]

Step 1: select two prime's *p* and *q*.

Step 2: calculate n= pxq

Step 3: calculate Ø (n) = (p-1) (q-1)

Step 4: select *e* such that *e* is relatively prime to Ø (n).

Step 5: calculate d such that d= mod (Ø (n))

Step 6: calculate c ; $C = M^e \bmod n$

Step 7: calculate $M = C^d \bmod n$.

Thus the obtained key is encrypted by using the RSA algorithm to send through the channel and finally it is digitally signed by using digital signature algorithm which is discussed in section below.

3.2.3 Digital Signature Scheme

A digital signature is an authentication mechanism that enables the creator of a key to attach a code that acts as a signature. The signature is formed by taking the hash of the key and encrypting the key. The signature guarantees the source and integrity of the key. The signing of a key is done by the private key of the user A [1]. For this purpose Elliptic Curve Digital Signature algorithm is adopted for signing a message m by sender S using A's private key, S_A. In this article the message is the secret key. So the concatenated and encrypted messages along with the values of r and s signature pair keys are sent through the channel. The receiver must decrypt and de-concatenate the message and does the verification process. The steps are as follows.

Step 1: e= h (m)

Step 2: select a random integer k from [1 n-1]

Step 3: calculate r =x1(mod n)

Step 4: s = (1/k)(e + SA x r)(mod n).

The signature pair is (r, s). The steps of verification for user B to authenticate user A are as follows,

Step 1: Verify whether r, s are in [1, n-1]

Step 2: Calculate e= hash (m)

Step 3: Calculate w=(1/s)(mod n)

Step 4: u1 = e x w (mod n) & u2 = r x w (mod n)

Step 5: Calculate (x1, y1) = u1x G + u2 x QA

Step 6: The signature is valid if x1 = r (mod n).

Thus the signature is authenticated and verified.

4 Simulation Results

Simulation is performed using NS-2 tool for the proposed HADS algorithm in the AODV protocol [11] with and without the presence of black hole attack. The performance metrics such as end to end delay, packet delivery ratio, throughput and overhead are analyzed and obtained. The simulation parameters are tabulated.

Table1 Simulation parameters

Simulation Time	20 minutes
Terrain Area	750X750 m^2
Number of Nodes	100
Node Placement Strategy	Random
Propagation Model	Two-Ray Model
Mobility Model	Random way point
Network Protocol	MAC/802-11
Routing Protocol	AODV

4.1 End to End Delay

End-to-end delay is defined as the time taken for a packet to be transmitted across a network from source to destination. It involves processing delay, queuing delay etc. By varying the number of nodes from 0 to 20, with the black hole attack the delay obtained is greater. On applying the HADS scheme in the RREQ and RREP packet of each transmission and reception, the delay obtained is very less. Similarly by varying the nodes to 50 and 100, the delay obtained is less, which implies that, for any number of nodes the delay in HADS scheme is lesser compared to with BHA. It is observed that the delay obtained is 68% less for 20 nodes, 60% less for 50 nodes, and 61% less for 100 nodes. This shows that the probability of attack is less by applying HADS scheme which is shown in fig 4.1, fig 4.2 and fig 4.3

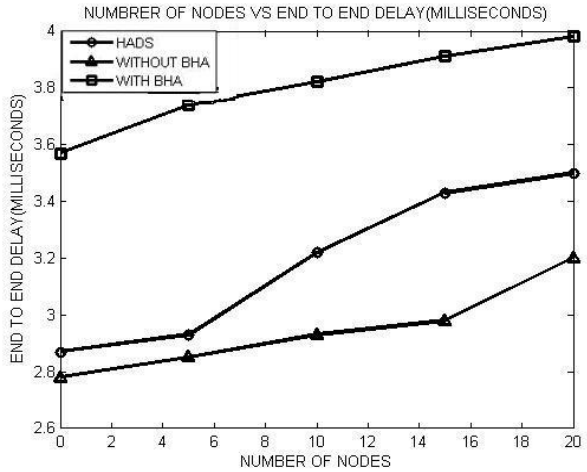

Fig.4.1 Number of nodes (20) vs. end to end delay (milliseconds)

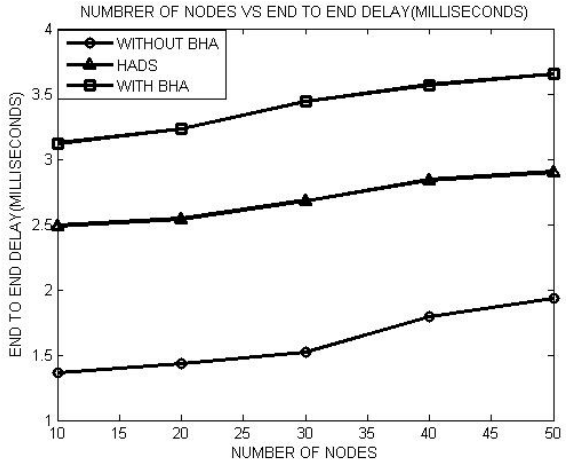

Fig.4.2 Number of nodes (50) vs. end to end delay (milliseconds)

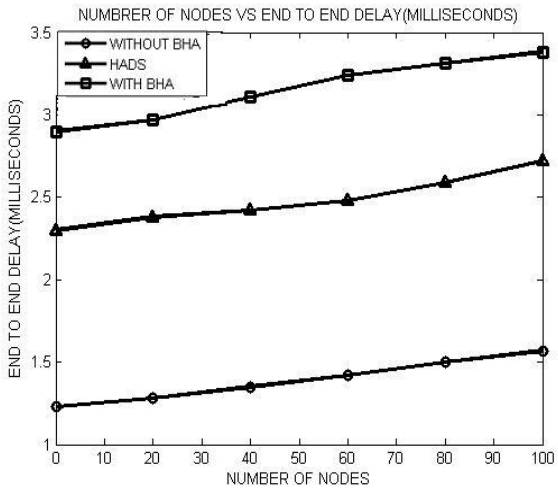

Fig.4.3 Number of nodes (100) vs. end to end delay (milliseconds)

4.2 Packet Delivery Ratio

Packet delivery ratio is defined as the ratio number of packets received to the number of packets sent. If there is a black hole attack there will be loss of packets at each transmission and reception, hence there will be loss of information. On applying the HADS scheme, the information before receiving and sending is completely authenticated and verified. Hence there is no way of losing the information. So the number of packets sent and received is same without any loss. So the packet delivery ratio is more when compared to other schemes. By considering 20, 50, 100 nodes the packet delivery ratio obtained is more. So for any number of nodes the packet delivery ratio is more. This is shown by fig 4.4, fig 4.5, and fig 4.6. It is observed that the packet delivery ratio in the presence of black hole attack is less. After applying the HADS scheme the packet delivery ratio is increased by 20 % for 20 nodes, 21 % for 50 nodes and 21% for 100 nodes. This shows that HADS scheme eliminates the black hole attack.

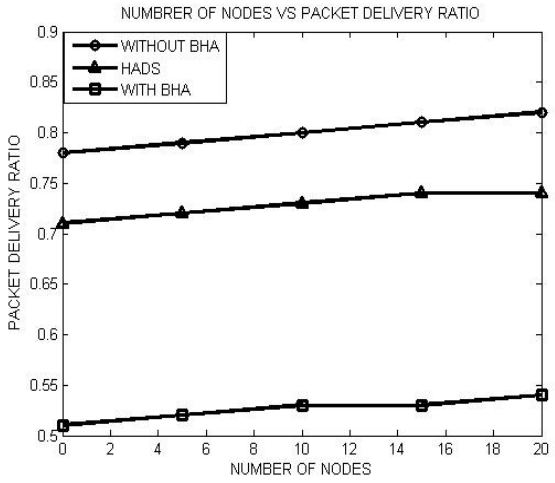

Fig. 4.4 Number of nodes (20) vs. packet delivery ratio

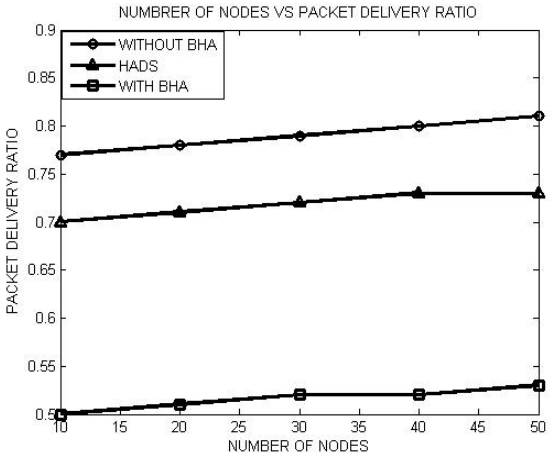

Fig. 4.5 Number of nodes (50) vs. packet delivery ratio

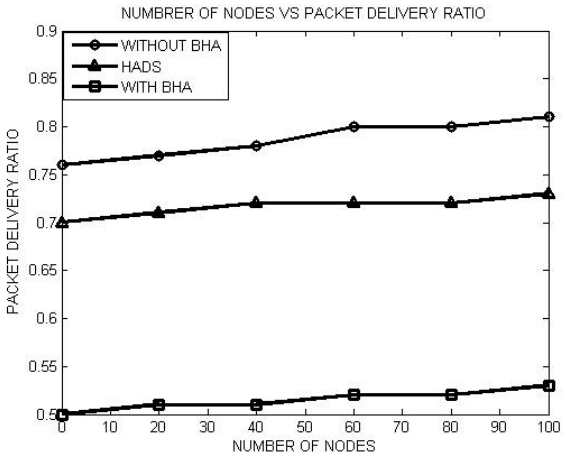

Fig. 4.6 Number of nodes (100) vs. packet delivery ratio

4.3 Overhead

Overhead is the amount of resources lost in the network and due to the computational complexities. In the presence of black hole attack the overhead is more. But in HADS scheme though mathematical computations are included in HADS scheme overhead is reduced and is lesser compared to with BHA. On varying the number of nodes 20, 50 and 100, the overhead is obtained as 10%, 11 %, 10% lesser compared to with BHA. This is shown in the figures 4.7, 4.8, and 4.9

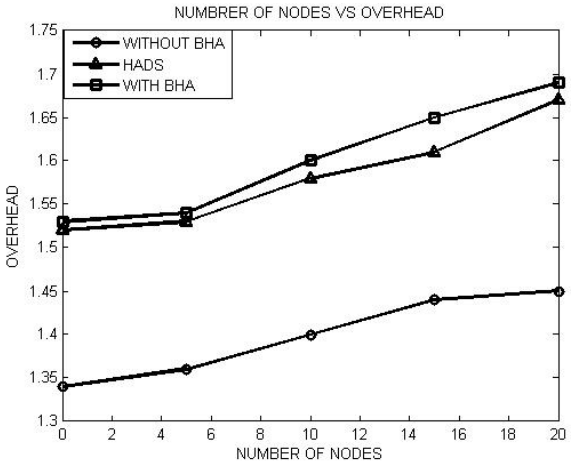

Fig. 4.7 Number of nodes (20) vs. overhead

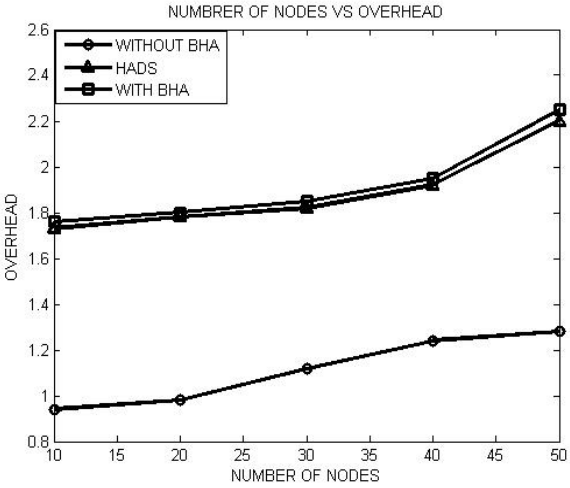

Fig. 4.8 Number of nodes (50) vs. overhead

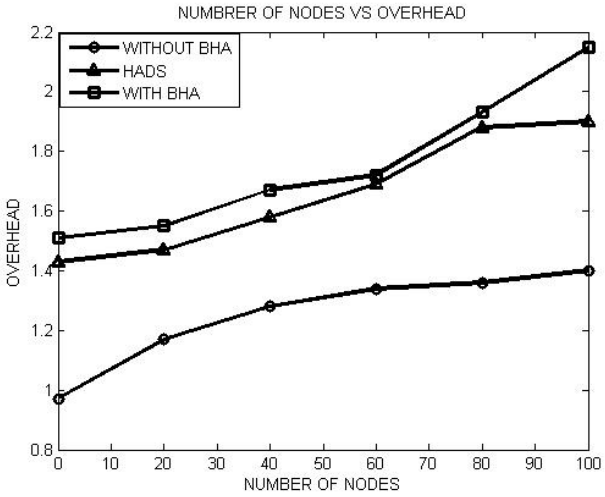

Fig 4.9 Number of nodes (100) vs. overhead

4.4 Throughput

The number of attackers is increased in each stage and the throughput and delay are analysed. Throughput is calculated as the ratio of the output in bits to the difference in time of the first packet sent and the last packet received. It is measured in bits per second. On applying the HADS scheme the throughput obtained is greater and the delay obtained is comparatively less. This can be shown in the fig 4.10 and fig 4.11. From the simulation results it is observed that throughput with HADS increases by 10%, delay decreases by 20% by increasing the number of attackers.

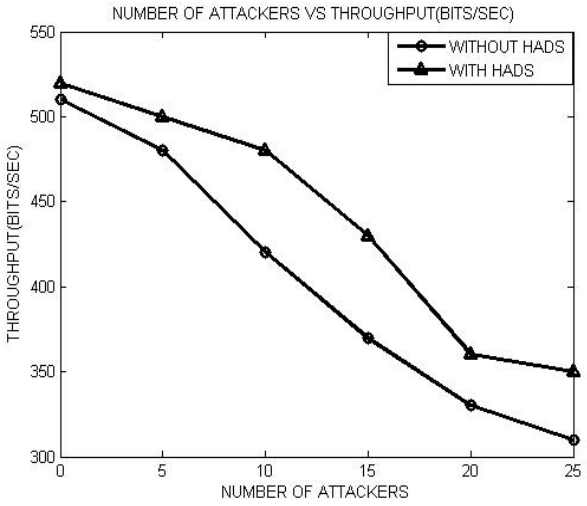

Fig.4.10Number of attacker's vs. throughput

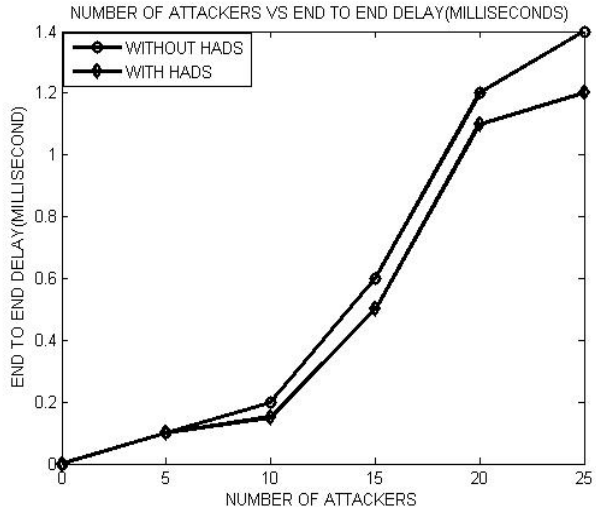

Fig 4.11 Number of attackers vs. end to end delay (millisecond)

4.5 Node speed vs. Delay, Packet Delivery Ratio and Throughput

The node speed is varied from 0 to 50 m/s and the delay, packet delivery ratio and throughput metrics are calculated. With HADS scheme, the black hole attack is eliminated and the delay is thereby decreased, the throughput and packet delivery ratio are greater when compared to the absence of the HADS scheme. This is shown figs 4.12, 4.13 and 4.15. The simulation results shows that delay decreases to 50%, packet delivery ratio increases to 20% and throughput increases to 10%. Though the node speed increases, the performance does not get affected in HADS scheme.

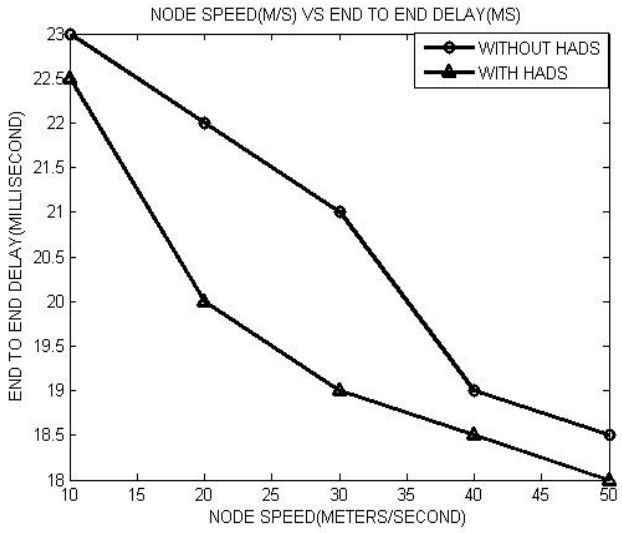

Fig 4.12 Node speed (m/s) vs. end to end delay

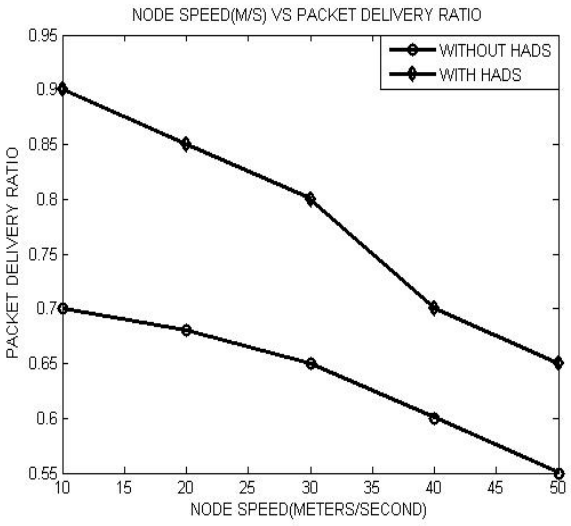

Fig 4.13 Node speed(m/s) vs packet delivery ratio

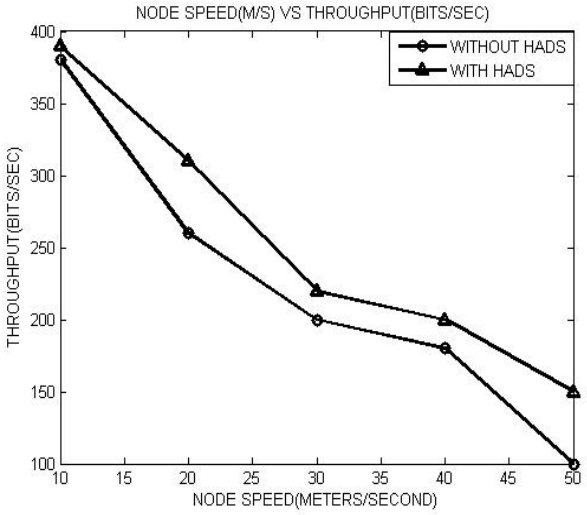

Fig 4.14 Node speed (m/s) vs. throughput (bits/sec)

4.6 Comparison of HADS algorithm with NRMT for 50 nodes with and without Black hole attack

4.6.1 Packet Delivery Ratio

The packet delivery ratio for HADS algorithm is better than NRMT and with BHA attack. This shows that HADS algorithm produces better security than NRMT.

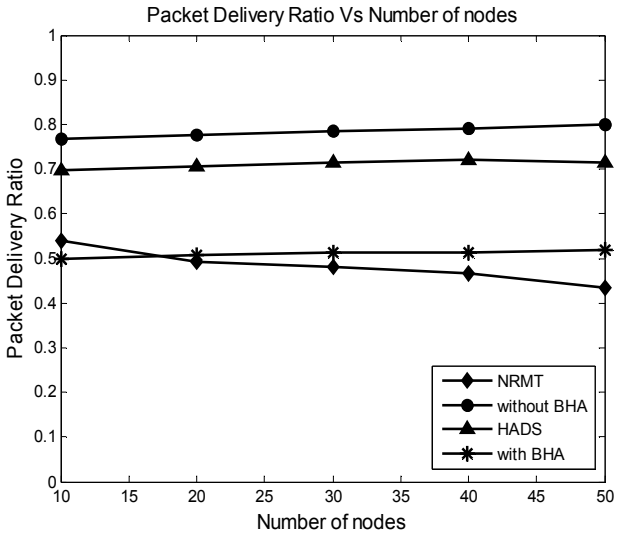

Fig. 4.15 Number of nodes (50) vs. packet delivery ratio

4.6.2 End to end delay

The end to end delay of our proposed algorithm HADS shown in fig 4.2 is lesser compared with BHA attack and the NRMT algorithm shown in figure 4.16 below. This shows the better performance of HADS algorithm.

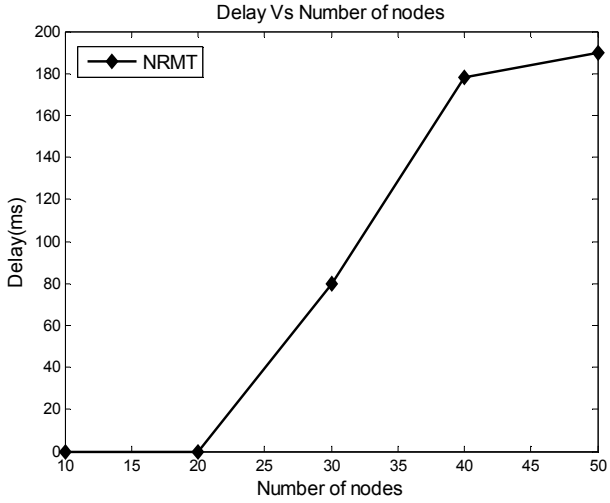

Fig. 4.16 Number of nodes (50) vs. end to end delay

4.6.3 Routing Overhead

The routing overhead of the proposed algorithm HADS is lesser compared to NRMT and with BHA attack. This is mainly due to the secret key generation using ECC in HADS scheme.

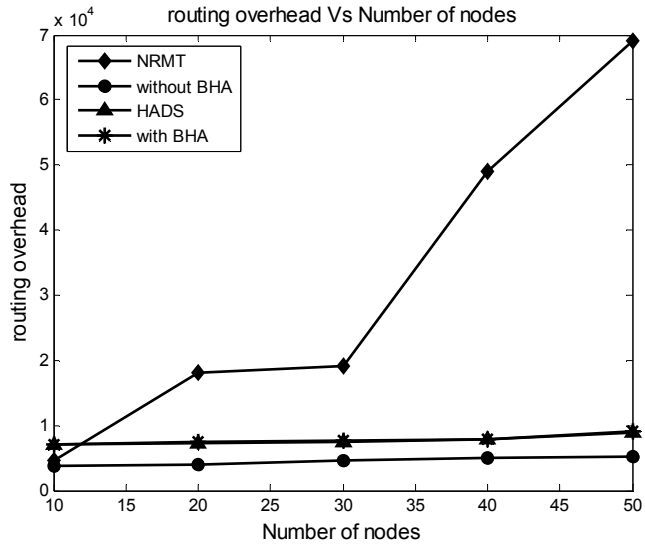

Fig. 4.17 Number of nodes (50) vs. Routing Overhead

5 Conclusion

In this article the security is provided by two schemes namely the elliptic curve cryptography and the digital signature algorithm. Various points are generated from the elliptic curve of prime field and a point is chosen at random. When a set of nodes are ready to form a MANET, they authenticate and communicate with each other by using the private and public keys. The keys for the users are generated using the elliptic curve equation. Now the secret key to be shared is encrypted using the RSA algorithm. The keys before sending and receiving must be signed at the sender and verified at the receiver. For authentication purpose elliptic curve digital signature algorithm is adopted. So the concatenated and the encrypted key along with the signature pair key are sent through the channel. The receiver decrypts and de-concatenates the secret key and does the verification process. Thus a new scheme, HADS comprises of hashing the keys and the implementation of digital signature algorithm for verification and authentication. The security is thus enhanced at various levels which prevent strong malicious attacks. In the existing method security is obtained by identity based scheme [2]. In this article instead of using identity based scheme, HADS scheme is implemented. The performances metrics such as packet delivery ratio, end to end delay, overhead and throughput are analysed with and without the presence of black hole attack in the AODV protocol. The results are also compared with another secured HRMT algorithm [18]. The performance metrics such as packet delivery ratio, end to end delay, overhead and throughput shows very good results when compared with HRMT algorithm. This proves that HADS scheme is highly secured.

6 Future Work

In future a trust based scheme [17] can be used, in which the topology is simplified by allowing only the trusted nodes to participate in the network which reduces the number of keys used and also the overhead. But such scheme is necessary for high security reasons in MANETs. Such security system is used in military and battle field. It is deployed for both surveillance and combat operations and has brought about the need for a large amount of data transfer between command centers and the edge of the tactical communication network. The technology at present demands renewed attention owing to recent developments in radio communications and advancements in wireless networking.

References:

[1] William Stallings, “Cryptography and network Security”, 5th edition, 2012, pp. 310-318.

[2] Wan An Xiong, Yao Huan Gong, “Secure and Highly Efficient Three Level Key Management Scheme for MANET”, proceedings of WSEAS transactions on computers, Volume 10, 2011, pp. 6-15.

[3] Maria Celestin Vigila S, Muneeswaran K, “Implementation of Text based Cryptosystem using Elliptic Curve Cryptography”, IEEE, Volume 9, 2009, pp. 82-85.

[4] Durgesh Wadbude, Vineet Richariya, “An Efficient Secure AODV Routing Protocol in MANET”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, 2012, pp. 274-279.

[5] Prakash Kuppuswamy, Peer Mohammad Appa, Dr. Saeed Q Y Al-Khalidi, “A New Efficient Digital Signature Scheme Algorithm based on Block cipher”, IOSR Journal of Computer Engineering (IOSRJCE), Volume 7, Issue 1, 2012, pp. 47-52.

[6] Bin Sun and Bin Yu, “The Three-Layered Group Key Management Architecture for MANET”, proceeding of 11th International Conference Volume 02, 2009, pp. 15-18.

[7] Fiat A and Shamir A, “How to Prove Yourself: Practical Solutions to Identification and Signature Problems” proceedings of the Springer-Veriag, 1999, pp. 306-314.

[8] Menezes A, Okamoto T and VanstoneL S, “Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field”, journal of information theory, IEEE transaction, Volume 39, 1991, pp. 1639-1646.

[9] Nishu Garg, Mahapatra R.P, “MANET Security Issues”, IJCSNS International Journal of Computer Science and Network Security, Volume 9, 2009, pp. 1-4.

[10] Haiyun Luo, “URSA Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks”, IEEE/ACM transactions on networking, Volume 12, No. 6, 2004, pp. 1049-1063.

[11] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, “Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic

Learning Method", International Journal of Network Security, Volume 5, No.3, 2007, pp.338–346.

[12] Jin-Hua Hong, Wei-Chung Wu, "The Design of High Performance Elliptic Curve Cryptographic", IEEE, Volume 9, No.9, 2009, pp. 527-530.

[13] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), Volume 1, 2012, pp 269-275.

[14] Himadri Nath Saha , Debika Bhattacharyya , Banerjee, "A Distributed Administration Based Approach for Detecting and Preventing Attacks on Mobile Ad Hoc Networks", International Journal of Scientific & Engineering Research, Volume 2, Issue 3, 2011.

[15] Mamatha G.S, Sharma S.C, "A Highly Secured Approach against Attacks in MANETS", International Journal of Computer Theory and Engineering, Volume 2, 2010, pp. 815-819.

[16] Elizabeth. M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks", IEEE Personal Communications, 2009, pp. 46-57.

[17] Edna Elizabeth, Radha. S, Priyadarshini. S, Jayasree. S, Naga Swathi. K, "SRT-Secure Routing using Trust Levels in MANETs", European Journal of Scientific Research, Vol.75 No.3, pp. 409-422, 2012.

[18] Arunmozhi Annamalai, Venkataramani Yegnanarayanan, "Secured System against DDos Attack in Mobile Adhoc Network", issue 9, volume 11, pp 331-341, 2012