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

HYBRID BASED ROUTING ALGORITHMS TO REDUCE THE ATTACKS AND IMPROVED SECURITY ALGORITHM IN MANET

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

The main objective of this paper is to study about various cryptographic techniques such as modified ECC and DSA based ECGDSA to enhance the data transfer security within the MANET systems. Both the algorithms will exhibit with the key size of 512 bits. The research in this paper is carried out.

To analyze various challenges of MANETs based on their issues in key size generation, time taken for key generation, packet delivery ratio and its throughput. To compare and investigate the performance of various hybrid algorithms such as RSA, ECC and modified ECC and DSA based ECGDSA.

To reduce the DoS attacks based on secure hybrid authentication protocol. MANET is a self configurable network of mobile routers connected without wires. MANET nodes cooperate to provide many wireless services and connectivity. The application program of this wireless network topology is restricted due on certain mobile ad hoc characteristics. MANETs are faced with certain attacks or threads due to lack of centralized operation.

.

Keywords: MANET (Mobile Ad hoc NETwork), multi hop network, ECKCDSA (Elliptic curve Korean Certificate Based Digital Signature Algorithm), The Blind Digital Signature (BDS).

1. INTRODUCTION

Based on the vulnerability of mobile ad hoc networks MANETs exhibit certain other attacks namely worm hole attack, black hole attack and sinkhole attack and DoS attacks.

These attacks will arise due to misbehavior functionality of nodes with various descriptive possibility in parameters based on evaluation. Various hybrid based routing algorithms which can reduce these attacks are ECKDSA SHA-512 and BDS on ECGDSA 512 etc. To evaluate the performance of the proposed algorithms, various new other algorithms like RSA and ECC cryptographic techniques are compared for the analysis.

The RSA algorithm is one form of highly secure public key algorithm which reduces the overall computational time of the key generation and verification. Certain attacks which arise with RSA algorithm are overcome by using ECC algorithm with smaller key lengths. The drawbacks of the ECC algorithm based on network overhead are reduced by using modified ECC algorithm. The modified ECC algorithm has reduced DoS attacks with good performance in packet delivery ratio.

The BDS on ECGDSA 512 is a encryption algorithmic technique which reduces the key length and computational overhead of the systems

ECKDSA SHA 512 is a encryption algorithm which is used to protect the data transfer between the source and the destination. 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. As the user alone knows the key the authorized parties are only allowed to view the message other intruders cannot view the message as they do not know the private key values while generating the signature.

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

II. ALGORITHM EXPLANATION

The algorithm has two main process to get executed they are signature generation and signature verification. 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 Generation:

In the signature generation phase the message is initially computed as hash value through the hash function. Here SHA-512 is used to determine the hash value of the integers. Then with the private key the signature is generated. In order to protect the message from the attacks of other intruders the input data message should be computed with the hash value again. To verify the signature public key should be given with the valid hash value. In the next level the validity of the signature is verified with the functional random integer values. Then the secured data is sent to the receiver with the specified requirements.

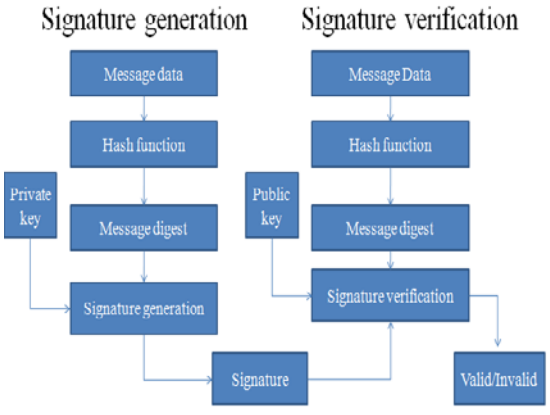

Fig 1: Flow diagram

III. RESEARCH METHODOLOGY

BDS on ECGDSA 512

Digital signature is used for identifying the owners of electronic data, thereby assures the traceability of electronic transactions. On the other hand, BDS disguises the content of a message from its signer, thereby assures the privacy of the users. The Blind Digital Signature (BDS) is one of the cryptographic techniques used with the ECGDSA algorithm. By using this algorithm the computational overhead is gradually reduced with the key size. BDS is a method of signing in such a way that the signer does not see the content of the document. Even if the signer sees the document he cannot determine for whom he has signed the document. This is equivalent to signing the document blindly. The BDS scheme usually will satisfy the following properties, they are correctness, blindness, unforgeability and unlinkability. The BDS scheme involves two parties; namely a "signer" and a signature "requester". The scheme allows the requester to have the message signed by the signer without revealing any information about the message. With a secure BDS scheme, the signer is unable to trace the signed message to the previous signing process, where the requester cannot be traced while using the signed message. For example, a bank can sign an electronic coin without seeing its serial number and later cannot distinguish this particular electronic coin from others. Since, customer's transactions cannot be traced, the privacy of the customer is ensured. BDS is used to provide user anonymity and unlinkability of electronic transactions, which prevents the signer from linking a blinded message he signed to the unblinded version that he may be asked to verify. The signed blinded message is unblinded prior to verification in such a way that the signature remains valid for the unblinded version of the message.

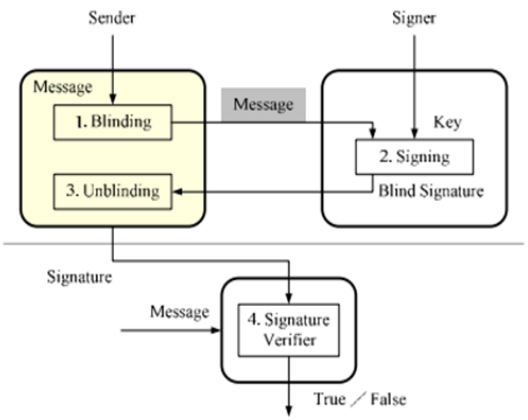

fig2: signature transaction

IV RESULTS AND DISCUSSION

This is a very important feature to ensure user privacy. By this way, BDS schemes can guarantee anonymity of the customers in secure electronic payment systems and privacy of the voters in secure electronic voting systems. According to Chaum's BDS scheme there are five phases: initialization, blinding, signing, unblinding, and verifying. And a BDS scheme must satisfy the following properties, they are:

Correctness: The correctness of the signature of a message signed through the proposed BDS scheme can be checked by anyone using the signer's public key.

Blindness: the content of the message should be blind to the signer.

Unforgeability: the signature is the proof of the signer, and no one else can derive any forged signature and pass through the verification.

Unlinkability: the signer of the BDS is unable to link the message/signature pair even when the signature has been revealed to the public.

Based on the above mentioned five basic properties the algorithm will be carried out with the five basic phases on key structure. The five phases of BDS based ECGDSA algorithms are,

- ✓ Initialization
- ✓ Blinding
- ✓ Signing
- ✓ Unbinding
- ✓ Verifying

Initialization Phase:

The signer defines the elliptical curve domain parameters T, defined in finite field F_p with integer specified basic parameters. Then for each request sended, the integer k is randomly selected by the user and the elliptical curve point R is calculated. To generate public and private keys the integer d is randomly chosen in the range of (1, n-1). The elliptical curve point is chosen based on the private key and the generator point.

Blinding Phase:

In the blinding phase to blind the message the owner of the message need the elliptical curve domain parameters. Those parameters are obtained with the following steps,

1. Sender sends the elliptical point R to the requester which is used as the blinding coefficient.
2. Requester calculates R and generates the blinded message m and sends it back to the signer for signing operation.

$$m = AH(m)r'r^{-1} (\mathrm{mod}\, n) \qquad (1)$$

Signing Phase:

After the signer receives the blinded message m from the requester, he generates the blind signature S.

$$s' = dr' + km' (\mathrm{mod}\, n) \qquad (2)$$

Unblinding Phase:

When the requester receives the blind digital signature S from the signer, the unblinding operation

is needed to obtain the digital signature (*s*, *R*) on message *m*.

$$s = s' rr^{r-1} + BH(m) \bmod(n) \qquad (3)$$

Verification phase:

Finally the Any party who has the elliptic domain parameters *T* of the signer can verify the digital signature of (*s*, *R*) on the message of m by following these steps by using public key of the signer, *Q*:

$$U_1 = sG(\bmod n)$$
$$U_2 = rQ + H(m)R \bmod(n) \qquad (4)$$

If the statement of U_1 and U_2 is met, then the signature is verified as valid, otherwise it is considered as invalid. Then the secured data is sent to the receiver with the specified requirements.

- This algorithm will be carried out in five major phases of initialization phase, binding phase, signing phase, unblinding phase and verification phase.
- Initially the sender will send the message to the blinding phase. In order to blind the message m the owner needs the elliptical curve domain parameters of the signer.
- After the signer receives the blinded message from the requestor the blind signature will be generated by the owner.
- When the requestor receives the blind digital signature from the signer the unblinding operation will generate the digital signature of the message.

The digital signature of the message will finally be verified based on the message using public key.

V CONCLUSION

The Hybrid and secure authentication protocol is proposed based on ECKCDSA SHA512 hash function and which improves the detection of the misbehavior nodes with the attacker by enhancing the system security. Using modified ECC algorithm, the packet delivery ratio is increased with decrease in computation overhead and key length.The computational overhead is also reduced with the use of BDS on ECGDSA 512 algorithm.

References

[1] 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.

[2] 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.

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

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

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

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

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

[8] 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.

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

[10] 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.

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

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

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

[14] 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.