COMPARITIVE STUDY ON ECKDSA SHA-512 AND BDS ON ECGDSA 512 ALGORITHMS FOR MANET USING IMPROVED ELLIPTICAL SECURITY

M.CHARLES AROCKIARAJ[1], DR.P.MAYILVAHANAN[2]
[1]Research Scholar, Vels University,Chennai. 600117, mcharles2008@gmail.com
[2]HOD,Dept.of MCA, Vels University,Chennai-600117,Tamil Nadu,INDIA.

ABSTRACT

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. 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 its 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).

OBJECTIVE OF THE STUDY

The main objective of this paper is to study and compare 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.

NEED FOR THE STUDY

Due to lack of unauthorized firewall techniques, MANET exhibit various attacks based on the security threads. To detect and reduce these threads various hybrid algorithms are proposed in this study. Certain attacks namely worm hole attack, black hole attack and few other DoS attacks are reduced based on the hybrid algorithms suggested in this study.

METHODOLOGICAL ANALYSIS OF THE STUDY

Based on the vulnerability of mobile ad hoc networks MANETs exhibit certain 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 overcomed 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 an encryption algorithmic technique which reduces the key length and computational overhead of the 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

COMPARITIVE ANALYSIS

TABLE 1: Analysis Table

Parameter Name	ECKDSA SHA 512	BDS on ECGDSA 512
Key Size	163	160
Time taken for key Generation	0.08	0.25
Encryption throughput	61.93 KBps	84.36 KBps
Decryption throughput	33.11 KBps	46.72 KBps
Blinding	5M+2H+1I	6M+1H
Signature	1M	0M
Verifying	2M+3H	3M
Packet delivery ratio	0.87	0.93

Here we show the comparison of the efficiency of our scheme with ECKDSA SHA 512 scheme and the results are shown in Table 1. Let I, H and M respectively denote the computational overhead for modular inverse operation (I), the hash operation (H) and the point multiplication (M). Each phase in the scheme has less computational load. Further the total computation cost in proposed BDS ECGDSA 512 scheme is 9M+ IH as compared to the ECKDSA SHA 512 scheme which is 7M+5H+ lI. In formulated scheme we have not introduced any modular inverse operation which is very costly in case of ECC. Our scheme contains only one hash operation whereas the ECKDSA SHA 512 scheme has many hash functions. Thus our proposed scheme is more efficient one.

CONCLUSION

In this research study, we put forward a secure and efficient blind signature scheme based on the Elliptic curve Discrete Logarithm Problem. This scheme utilizes fewer numbers of bits due to inherent property of elliptic curve as compared to its public key counterparts, such as, ECKDSA SHA 512 and DLP. The scheme also satisfies untraceability property. We have proved that the proposed scheme BDS on ECGDSA 512 is universally verifiable with watermarking functionalities. The scheme has low computational overhead and proved to be resistant against active attacks. The proposed scheme is suitable for applications, such as, e-banking, e-commerce and e-voting.

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] 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.

[4] 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.