Optimal ECC Based Hybrid Signcryption for MANET Security

Sujatha.R [1], Dr.Ramakrishnan.M[2]

[1]Anna University, Chennai, 600066 India.
[2]Madurai Kamaraj University, Madurai, 625021, India.

Abstract

In Mobile Ad hoc Network (MANET), to resolve the crisis in message confidentiality and authenticity , new hybrid algorithm is proposed based on Elliptic curve cryptography .Generally MANET's are vulnerable to attacks because of their open environment ,where all nodes are involved in the data transfer .To improve the performance in MANETs and to protect it from various attacks we propose a highly secured cryptographic protocol .This scheme aims to incorporate the best features of both digital signature and encryption schemes in a single step. Elliptic curve method is significantly efficient with reduced key size, and it is highly infeasible against Brute force attacks when compared with Advanced Encryption standard methods .As the key size is reduced which in turn curtails the memory constraints which is very much important in a resource constrained environment . The proposed work will help nodes to avoid vulnerable assaults within themselves and also aims to increase the performance of MANETs by averting malicious nodes. In this paper, Elliptic Curve cryptography is applied for data encryption. It also provides reliable and efficient transmission of data in a MANET, which will drastically reduce intruders within and outside the network.

Keywords: , Elliptic curve cryptography; Hybrid Signcryption ; Warm Hole attack; Grey Hole Attack; Denial of service attack; Authentication, Packet Delivery ratio, Distributed routing.

I. INTRODUCTION

Cryptography is one of the most important process in the MANET architecture, considering it's mobility, robustness and non-hierarchical architecture. A mobile ad hoc network (MANET) is a continuously self-configuring network, which does not have a fixed infrastructure. Security is a challenging issue in a dynamic topology like Adhoc networks, providing any secure communication protocol should satisfy the following security requirements, Mutual authentication , Confidentiality ,Data Integrity and Non Repudiation[1].The setup of the MANET consists of dynamically changing nodes that do not stay in the same communication range for a long period. It consists of many individual nodes communicating with each other nodes through wireless technology. MANETs are known for their open and dynamic infrastructure and are ad hoc in nature. This nature of these networks makes it more vulnerable to various attacks [2]. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. In other words, every node in a MANET acts both as a transmitter and a receiver. Due to their dynamic nature, nodes in a MANET misbehave and fail to co-operate with the other nodes during packet transmission. Due to this erroneous behavior the performance of the network may be reduced drastically. MANETs are capable of communicating with each other efficiently with the help of Ad hoc On-Demand Distance Vector protocol (AODV).Every node in a MANET has to maintain information to route traffic in the network. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. The MANET is well renowned for its simplistic infrastructure and mobility in its fields. However, these characteristics tend to produce a defective model. Being an open system, MANET is prone to numerous security attacks within its architecture. The main objective of this work is to employ a strong cryptographic technique to safeguard the data, which should be capable of improving confidentiality and authenticity of the data. It is also essential to improve the QoS even when it is under attack. At the same time security of the transmitted data is also taken into consideration. Therefore, proper measures in the renovation of QoS is mandatory, in order to gain better service in an attack-oriented environment. In the traditional existing security design for MANET, can provide either confidentiality or authenticity to the data[2]. But the problem lies in the increasing number of overheads while implementing advanced techniques. Such algorithms could trade-off the Quality of Service of the Mobile Adhoc Network to it's security constraints. Complex encryption algorithms tend to increase the key size as well as computational time. Hence, it could decelerate the data transfer process of the nodes, resulting in a decline in the QoS of the entire network.

A. Objective of the proposed work

With regard to have a secured Mobile Adhoc network, cryptographic archaic is integrated in each and every node. To enact the above objective Elliptic curve based cryptography is proposed. ECC based signcryption schemes are more decisive as it avoids massive bilinear operations .Each node transmits its information to the Broad casting node using the improved ECC based signcryption algorithm.

B. Related Work

Ze Li ,Shen 1] propose a QoS-Oriented Distributed routing protocol (QOD) to enhance the QoS support capability of hybrid networks. Results are based on the random way point model and the real human mobility model .

Jian Li, Yun Li [2] proposed a scalable authentication scheme based on elliptic curve cryptography (ECC). Proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem.

Significant research has been devoted by Sravana Kumar, C.H. Suneetha and A. Chandrasekhar [3] to support realime transmission with stringent Quality of Service (QoS) requirements for wireless applications.

Jian hong Zhang, Zhipeng Chen and Min Xu [4] discussed about hop by hop message authentication as one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. A ID based multi receiver scheme was introduced by Lei Wu [5] .However, this scheme and its extensions have the weakness of a built-in threshold determined by the degree of the polynomial, when the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial .

Prashant Kushwah and Sunder Lal [6] proposed an improved identity based signcryption scheme without random oracles. There are more literature work on certificate based public-key management in MANETs[7,8] in which public-key certificates are used. Jung- San Lee et.al[9] have proposed a protocol for cluster based ad hoc networks, using node identities to provide secure communication. Their protocol is based on identity based scheme.

Hyo Jin Jo [9] proposed protocol uses a pseudo-identity-based signcryption scheme to perform efficient revocation and efficient authentication. The use of signcryption algorithm in this work minimizes the number of pseudo-identities stored in a Subscriber Identification Module (SIM) card with limited storage capacity.

Yue-Hsun Lin ,Shih-Ying Chang, and Hung-Min Sun [10] proposed a new concealed data aggregation scheme extended from Boneh et al.'s homomorphic public encryption system.

Shohreh Honarbakh, Liza Binti ,Abdul Latif and Abdul Manaf [11] gave a certificateless solution which eliminates the need for public key distribution and certificates in public key management schemes.

II. IDEAL NETWORK ARCHITECTURE USING QOD ROUTING ALGORITHM

The basic architecture of our project is proposed through the implementation of QOD routing protocol (i.e.) Quality of Service Oriented Distributive routing protocol. By directly adopting resource .reservation based QoS routing for MANETs[12], it inherits invalid reservation and race condition problems in MANETs. The crucial factor for favoring this protocol over the available standardized AODV (Adhoc on Demand Distance Routing Protocol) is that, the proposed QOD routing protocol is advantageous and overcomes the short-comings of the present AODV routing protocol. QOD architecture incorporates five basic algorithms.

- QoS-Guaranteed Neighbour Selection Algorithm
- Distributed Packet Scheduling Algorithm
- Mobility-Based Packet Resizing Algorithm
- Soft-Deadline-Based Forwarding Scheduling Algorithm
- Data Redundancy Elimination

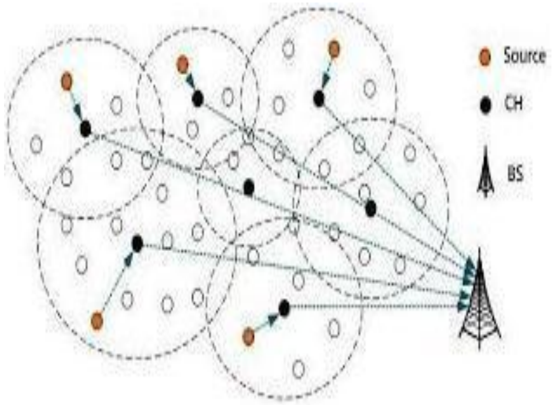

Fig. 1.QoD Architecture

The Basic architecture of the QOD routing protocol comprises of numerous mobile nodes and static access points as shown in the Fig.1.

The mobile nodes are the typical networking nodes that function as both source as well as the destination. The mobile nodes as prescribed are provided with mobility of desired levels. The access points are also networking nodes, which are made static and are configured with higher parameters in terms of transmission power, reception power, gain etc. The mobile nodes are assigned to send their packets to the access points for better services[13].The packets travel from different Access Points, which may lead to different packet transmission delay, resulting in a jitter at the receiver side. The jitter problem can be solved by using token buckets mechanism at the destination APs to shape the traffic flows.

We consider a hybrid wireless network with an arbitrary number of base stations spreading over the network [14]. A number of mobile nodes, say ‘n’ nodes are moving around in the network. Each node in the MANET uses IEEE 802.11 interface with Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol[15]. In a hybrid network where nodes are equipped with multi interfaces that transmit packets through multi channels generate much less interference than a hybrid network where nodes are equipped with a single WiFi interface, we assume that each node is equipped with a single WiFi interface in order to deal with a more difficult problem. Therefore, the base stations are considered as access points (APs)[16]. The WiFi interface enables nodes to communicate with both APs and mobile nodes. For example, in a University campus, normally only buildings have APs. Therefore, people that do not have WiFi access but close to buildings can use two hop relay transmissions to connect to the APs in the buildings.

A. QoS-Guaranteed Neighbour Selection Algorithm

As short delay is the major real-time QoS requirement for traffic transmission, QOD incorporates the Earliest Deadline First scheduling algorithm, which is a deadline driven scheduling algorithm for data traffic scheduling in intermediate nodes. In this algorithm, an intermediate node assigns the highest priority to the packet with the closest deadline and forwards the packet with the highest priority first.

B. Distributed Packet Scheduling Algorithm

In order to further reduce the stream transmission time, a distributed packet scheduling algorithm is proposed for packet routing. This algorithm assigns earlier generated packets to forwarders with higher queuing delays and scheduling feasibility. It also assigns more recently generated packets to forwarders with lower queuing delays and scheduling feasibility, so that the transmission delay of an entire packet stream can be reduced.

C. Mobility-Based Packet Resizing Algorithm

In a highly dynamic mobile wireless network, the transmission link between two nodes is frequently broken down. The delay generated in the packet retransmission degrades the QoS of the transmission of a packet flow. On the other hand, a node in a highly dynamic network has higher probability to meet different mobile nodes and APs, which is beneficial to resource scheduling. The basic idea is that the larger size packets are assigned to lower mobility intermediate nodes and smaller size packets are assigned to higher mobility intermediate nodes, which increases the QoS guaranteed packet transmissions.

D. Soft-Deadline-Based Forwarding Scheduling Algorithm

In the Earliest Deadline First scheduling (EDF) algorithm, an intermediate node forwards the packets in the order from the packets with the closest deadlines to the packets with the farthest deadlines. If an intermediate node has no problem to meet all packets deadlines in forwarding, that is, the packets are scheduling feasible, the EDF algorithm works satisfactorily. However, when an intermediate node has too many packets to forward out and the deadlines of some packets must be missed, EDF forwards out the packets with the closest deadlines but may delay the packets with the farthest deadlines. Therefore, EDF is suitable for hard-deadline driven applications (e.g., online conferences) where packets must be forwarded before their deadlines but may not be fair to all arriving packets in soft-deadline driven applications (e.g., online TV), where a missing deadline is sometimes acceptable. In order to achieve fairness in the packet forwarding scheduling for soft-deadline driven applications, a forwarding node can use the least slack first (LSF) scheduling algorithm.LSF can achieve more fairness than EDF. QOD can choose either LSF or EDF based on the applications and we can apply for LSF the same as EDF. The priorities of the packets are determined by the chosen policy.

III. DATA REDUNDANCY ELIMINATION

The mobile nodes set their Network Allocation Vector (NAV) values based on the overhearing message's transmission duration time. A large NAV leads to a small available bandwidth and a small scheduling feasibility of the mobile nodes. Therefore, by reducing the NAV value, we can increase the scheduling feasibility of the intermediate nodes and sequentially increase the QoS of the packet transmission. Due to the broadcasting feature of the wireless networks, in a hybrid network, the Access Points and mobile nodes can overhead and cache packets, we use an end-to-end traffic redundancy elimination (TRE) algorithm to eliminate the redundancy data to improve the QoS of the packet transmission in QOD. TRE uses a chunking scheme to determine the boundary of the chunks in a data stream. The source node caches the data it has sent out and the receiver also caches its received data. From the overhearing, the nodes know who have received the packets. When a source node begins to send out packets, it scans the content for duplicated chunks in its cache. If the sender finds a duplicated chunk and it knows that the AP receiver has received this chunk before, it replaces this chunk with its signature. When the AP receives the signature, it searches the signature in its local cache. If the AP caches the chunk associated with the signature, it sends a confirmation message to the sender and replaces the signature with the matched data chunk. Otherwise, the AP requests the chunk of the signature from the sender.

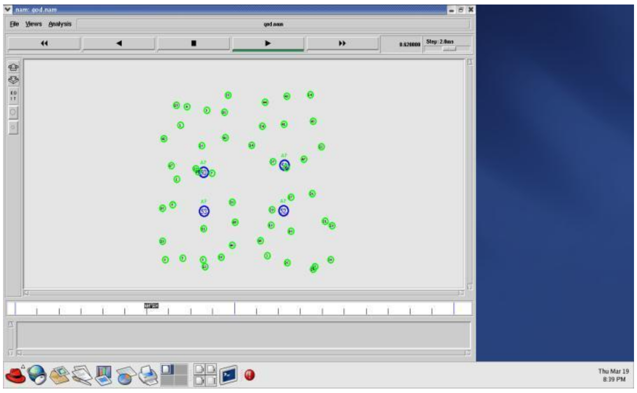

Fig.2. NAM of QoD routing protocol

A. Attacked Scenario

Denial of service (DoS) attacks have become a major threat to current computer networks. For example, an attacker might want to get control of an IRC channel via performing DoS attacks against the channel owner. Attackers could get recognition in the underground community via taking down popular web sites. The proposed security algorithm is best observed under this attack. Individual attackers can also exploit vulnerability, break into target servers, and then bring down services. Because it is difficult for attackers to overload the target's resource from a single computer, many DoS attacks were also launched via a large number of distributed attacking hosts in the Internet.

B. Wormhole Attack

In a wormhole attack an adversary records the information at an origin point, tunnels it to a destination point, and retransmits the information in the neighbourhood of the destination. Since a wormhole attack can be launched without compromising any node, the success of the attack is independent of the strength of the cryptographic method that protects the data. Hence, a wormhole attack is implemented with few resources and is difficult to detect. To launch a wormhole attack, an adversary establishes a direct link referred as wormhole link between two points in the network. Once the wormhole link is operational, the adversary eavesdrop messages at one end, referred as the origin point ,tunnels them through the wormhole link and replays them in a timely fashion at the other end. In the wormhole model, it is assumed that the adversary does not compromise the integrity and authenticity of the communication, and any cryptographic quantity remains secret .If an adversary had access to cryptographic keys, it could generate and forge any authentic message, and inject it back into the network .

C. Grey Hole Attack

The malicious node can accomplish this attack selectively, e.g. by dropping packets for a particular network destination. This is called a gray hole attack. When other nodes notice that the compromised node is dropping all traffic, they will generally begin to remove that node from their forwarding tables.. The packet drop attack can be frequently deployed to attack wireless ad hoc networks. By doing this, all traffic will be directed to the host that has been compromised, and the host is able to drop packets. Also over a mobile ad hoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network.

IV. PARAMETERS CONSIDERED

To monitor the data transfer in the presence of attacks, we measure two parameters such as Delay and packet loss ratio. These parameters indicate whether a user is achieving the QoS requirements. Here, delay is the end-to-end latency; packet loss ratio is defined as the ratio of number of dropped packets from a flow to the total number of packets of the same flow entered the domain. Delay and loss ratio are good indicators for the current status of the domain. This is because, if the domain is properly provisioned and no user is misbehaving, the flows traversing through the domain will not experience high delay or loss ratio. However, the above said two attacks are instrumental in affecting the QoS parameters (delay, throughput, PDR, jitter, energy etc.).

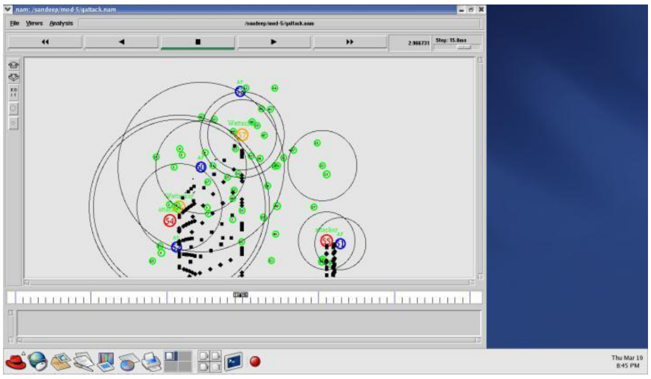

Fig.3. Attacked Network

V. PROPOSED ELLIPTIC CURVE CRYPTOGRAPHY BASED SIGNCRYPTION

By the foreseen cases, the MANET network is described as an architecture for achieving better QoS. The MANET network is shown to have enhanced it’s QoS parameters by implementing the proposed ECC based hybrid signcryption algorithm. Then, the network is subjected to Denial-of-service (DOS) attack, a security attack which is responsible for high degree of packet loss and increase in the transmission delay or latency. ECC hybrid signcryption cryptographic technique is employed to renovate the attacked scenario and to generate a private and public key for the encryption. ECC outperforms other encryption algorithms in terms of reduced key length, tight security, high speed, reduced memory space, computational cost and forward secrecy. The private and public keys generated by the ECC method are optimal.

A. Significance of Signcryption

In cryptography, signcryption is a public-key primitive that simultaneously performs the functions of both digital signature and encryption[18]. Encryption and digital signature are two fundamental cryptographic tools that can guarantee the confidentiality, integrity, and non-repudiation. Until 1997, they were viewed as important but distinct building blocks of various cryptographic systems. In public key schemes, a traditional method is to digitally sign a message then followed by an encryption (signature-then-encryption) that can have two problems: Low efficiency and high cost of such summation, and the case that any arbitrary scheme cannot guarantee security. Signcryption is a relatively new cryptographic technique that is supposed to fulfill the functionalities of digital signature and encryption in a single logical step and can effectively decrease the computational costs and communication overheads in comparison with the traditional signature-then-encryption schemes.

B. Implementation of Signcryption

The signcryption algorithm is applied through the padding of hash, which is generated from the digital signature. The hash padded data is then attached with a certificate from the digital signature, to the encrypted hash function. This forms the digitally signed data. It accounts for the authentication of the data among the peers. Then the signed data packet is subjected to encryption through the Chaining Block Cipher (CBC). In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.CBC has been the most commonly used mode of operation. Its main drawbacks are that encryption is sequential (i.e., it cannot be parallelized), and that the message must be padded to a multiple of the cipher block size. One way to handle this last issue is through the method known as ciphertext stealing. Note that a one-bit change in a plaintext or IV affects all following ciphertext blocks. An initialization vector (IV) or starting variable (SV) is a block of bits that is used by several modes to randomize the encryption and hence to produce distinct ciphertext even if the same plaintext is encrypted multiple times, without the need for a slower re-keying process.

C. Significance Of Hybrid Cryptosystem

In cryptography, public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely (among other useful properties). However, they often rely on complicated mathematical computations and are thus generally much more inefficient than comparable symmetric-key cryptosystems. In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive. A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. If both the key encapsulation and data encapsulation schemes are secure against adaptive chosen ciphertext attacks, then the hybrid scheme inherits that property as well. A hybrid cryptosystem can be constructed using any two separate crypto systems: a key encapsulation scheme, which is a public-key cryptosystem, and a data encapsulation scheme, which is a symmetric-key cryptosystem.

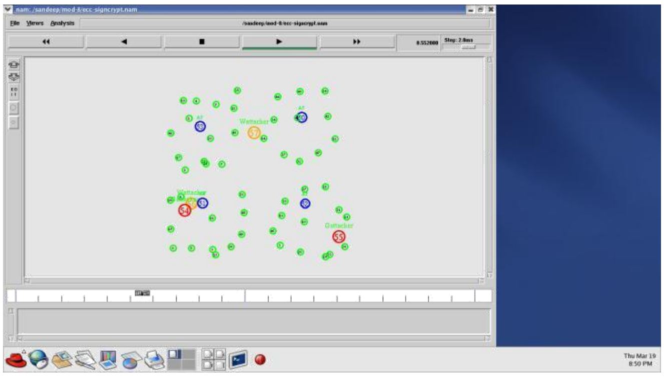

Fig. 4. NAM Screen shot f Proposed Algorithm

D. Significance of Elliptic Curve Cryptography(ECC)

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible: this is the "elliptic curve discrete logarithm problem" or ECDLP. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem.

E. Implementation of ECC Protocol

Our ultimate aim is to build the optimal signcryption based on KEM and DEM, the KEM is performed based on the key derivation function (KDF) using the secure pseudo random number generation technique. The KEM algorithm is used for transferring the secret symmetric key; to share the secret key the additional key will be required for different cryptographic reason such as encryption process, integrity protection algorithm. For this purpose here, we used the key derivation function to derive secret key from any other key or known information using the secure pseudo-random number functions. The various properties of KDF, functionality of pseudo-random number generator and the key expansion function. In conventional signcryption algorithm, the DEM is performed based on the AES encryption algorithm. In our proposed method, the AES algorithm is replaced by optimal Elliptic Curve Cryptography (ECC) algorithm.

Here in the signcryption algorithm, we have utilized an ECC method to create a private and public key for the encryption process. The private and public keys are generated by the ECC method makes the data more secure for embedding and also the generated keys are robust.

The operations of elliptic curve cryptography are defined over two finite fields: Prime field and Binary field. The suitable field is selected with finitely huge number of points for cryptographic operations. The prime field process operates by choosing a prime number, and finitely large numbers of basic points are generated on the elliptic curve, such that the generated points are between 0 to Z.

F. ECC Based Signcryption Algorithm

- Align all the data packets to be passed during the timed session.
- Perform XOR operation on the plain text using the digital signature (static) as the Initialization Vector.
- Perform Symmetric key encryption using Chaining Block Cipher mode of operation, to obtain the Cipher Text.

  $\text{Cipher\_text1}=\text{CBC}\ (\text{Plain\_text1}\oplus\text{Digial\_signature\_no})$
- Use the Cipher text of first packet to perform the XOR operation on the successive packet.

  $\text{Cipher\_text2}=\text{CBC}\ (\text{Plain\_text2}\oplus\text{Cipher\_text1})$
- Repeat the process for all the packets to be transferred in the session.

  $\text{Cipher\_text}_i= \text{CBC}\ (\text{Plain\_text}_i\oplus\text{Cipher\_text}_{i-1})$
- Pad the symmetric key with the data packet, after each iteration process
- Encrypt the key padded data packet using Asymmetric key cryptography of ECC

Table 1. Comparison of all protocols with proposed ECC based signcryption with respect to Packet Delivery Ratio (PDR)

Time (µSeconds)	Delay (µseconds)				
	AODV	QOD	Attacked scenario	Signcryption	Proposed ECC based Signcryption
2	1466.13	0	31.67	105.13	0
4	2048.45	14.32	789.28	116.10	13.14
6	2351.82	31.57	1421.17	120.75	14.04
8	1762.82	46.46	1989.14	122.61	14.81
10	1394.26	95.90	2390.39	123.10	15.79

Table 2. Comparison of all protocols with proposed ECC based signcryption with respect to Packet Delivery Ratio

Time (µseconds)	Packet Delivery Ratio (bits)				
	AODV	QOD	Attacked scenario	Signcryption	Proposed ECC protocol
2	0.9755	0	0.0008	0.0233	0.137
4	0.7654	0.3889	0.0094	0.3140	0.3889
6	0.6650	0.6381	0.0098	0.4167	0.4333
8	0.4714	0.6711	0.0097	0.4762	0.5000
10	0.4448	0.6058	0.0087	0.4941	0.5517

- Perform both Key Encapsulation Mechanism and Data Encapsulation Mechanism on data packet.

Packet Delivery Ratio is the ratio of Packets received to packets sent. Confidentiality and integrity of the data packets has to be assured even in the presence of malicious nodes. Novel ECC based protocol by reducing the delay, packet delivery ratio can be improved .ECC based signcryption can perform better when compared with other conventional methods.

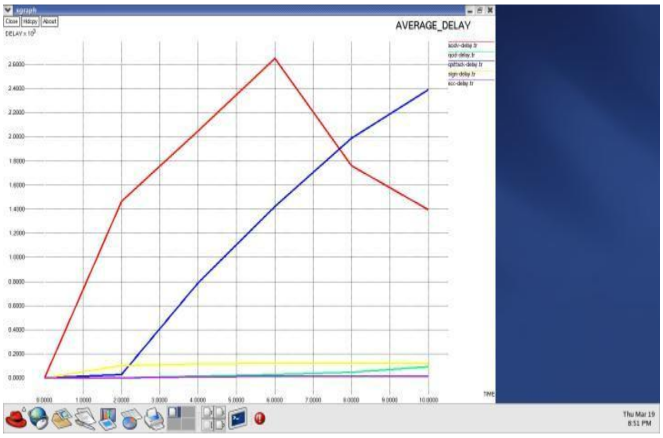

Fig.5. Delay Graph for the proposed ECC based Signcryption.

Comparison has been done for the existing protocols in the system. The graph compares the performances of the applied algorithm in terms of run time (seconds) that has been mentioned in Table 1. Being the default routing protocol, AODV is taken into consideration in terms of delay. It is drawn into comparison with QOD routing protocol. QOD routing protocol due to it's QoS enhancing algorithms during data transfer, produces the lowest delay reading to be recorded. Thus, it can be termed as the idealistic realization of the MANET system or architecture.

The QOD implemented MANET architecture is then implemented with the DoS attacks (namely Gray hole attack and Wormhole attack). Due to the behaviour of these malicious nodes, high degree of packet drop is observed in this system. Thus, the delay as a result is significantly increased. It describes the worst-case scenario of the system, where the performance of the system is at it's lowest.

To counteract these DoS attacks, the renovated scenario is implemented in two stages. First, the Signcryption is implemented and thus, it introduces the data confidentiality and authenticity of the data packet. By counteracting the malicious nodes, the delay in the network is significantly reduced, near to that of QOD routing protocol.

Next, the ECC protocol is implemented into the Signcrypted data packet. By the ECC protocol, the routing of the packet occurs based on the detection of the nodes within it's elliptic curve. This implementation of ECC is beneficial in the reduction of the delay, to the order of the QOD routing protocol.

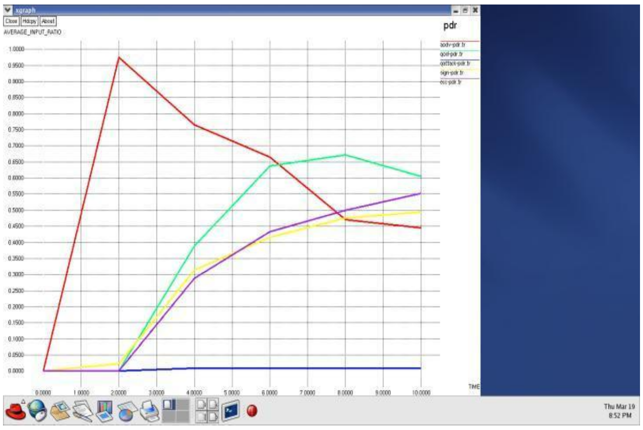

Fig.6. Packet delivery ratio for the proposed ECC based signcryption

Table 3 : Comparison of security parameters

Protocol	Security parameter			
	Confidentiality	Authentication	Data integrity	Non repudiation
QOD protocol	Nil	Nil	+	Nil
QOD under attack	-	--	--	--
Signcryption	+	+	+	+
Proposed ECC based signcryption.	++	+	++	+

Table 3 shows the security of the proposed protocol is greatly enhanced when compared with the other applicable algorithms. Table 4 gives the explanation for the symbols used

Table 4. Legend for security parameters

+	Enhanced
++	Greatly enhanced
-	Deteriorated
--	Greatly deteriorated

VI. CONCLUSION

The proposed ECC protocol enhances the security architecture of MANET. This scheme is realized as a more secured and confidential structure with improved network performance. In addition to the enhanced security by implementation of the ECC based cryptography algorithm, memory requirements for a resource constrained environment gets reduced as key size reduces. In the future, this work can be extended by enhancing ECC as hyper ECC in order to have reduced key size and tighter security. The general idea is to explore venues where the performance and the security of MANETs can be enhanced.

REFERENCES

[1] ZeLi, Haiying Shen, A QoS-Oriented Distributed Routing Protocol for Hybrid Wireless networks, IEEE Transactions On Mobile computing,2014.

[2] Jian li, Yun li, Jian ren, Hop-by-hop message authentication and source privacy in wireless sensor networks, IEEE Transactions on parallel and distributed systems, 2014.

[3] D. Sravana Kumar, CH. Suneetha and A. Chandrasekhar, Encryption of data using Elliptic Curve over Finite Field||, IJDPS, Vol. 3, No. 1, 2012.

[4] Jian hong Zhang, Zhipeng Chen, Min Xu "On the Security of ID-based Multi-receiver Threshold Signcryption Scheme", In proceedings of 2nd International Conference on Consumer Electronics, Communications and Networks ,(CECNet), pp. 1944 – 1948, 2012.

[5] Lei Wu, "An id-based multi-receiver signcryption scheme in MANET", Journal of Theoretical and Applied Information Technology, Vol. 46 No.1, pp. 120-124, dec-2012.

[6] Prashant Kushwah and Sunder Lal, "Provable secure identity based signcryption schemes without random oracles", International Journal of Network Security & Its Applications (IJNSA), ISSN: 0974 – 9330, Vol.4, No.3, pp. 97-110, May 2012.

[7] Yixin Jiang, Chuang Lin. Minghui Shi, Xuemin Shen, Xiaowen Chu, A DoS and fault tolerant authentication protocol for group communications in Ad hoc networks, Computer Communications, 2007 Vol.30, 2428-2441.

[8] Amit Gaur, Abhinav Prakash, Saugat Joshi, Dharma P. Agarwal, Polynomial based scheme (PBS) for establishing Authentic Associations in Wireless Mesh Networks ,Journal of Parallel and Distributed Computing ,Volume 70, Issue 4, 2010, 338–343.

[9] HyoJin Jo, Jung Ha Paik and Dong Hoon Lee, Efficient Privacy-Preserving Authentication in Wireless Mobile Networks, IEEE Transactions On Mobile Computing,2014.

[10] Yue-Hsun Lin, Shih-Ying Chang, and Hung-Min Sun, CDAMA: Concealed Data Aggregation Scheme for Multiple Applications in Wireless Sensor Networks, IEEE Transactions On Knowledge And Data Engineering,2013.

[11] Shohreh Honarbakh, Liza Binti ,Abdul Latif and Abdul Manaf ,Enhancing Security for Mobile Ad hoc Networks by using Identity Based Cryptography, International Journal of Computer and Communication Engineering,2014.

[12] Ramya K, Beaulah David, Shaheen ,Hybrid Cryptography Algorithms for Enhanced Adaptive Acknowledgment Secure in MANET,IOSR ,Journal of Computer Engineering,2014.

[13] Masayuki Abe, Rosario Gennaro and Kaoru Kurosawa, Tag-KEM/DEM: a New Framework for Hybrid Encryption and a New Analysis of Kurosawa-Desmedt KEM, Eurocrypt, 2005, 128- 146.

[14] Aumasson, J.P., Henzen, L., Meier, W., Naya Plasencia, M. Quark: A Lightweight Hash., Lecture Notes in Computer Science, vol. 6225, pp. 1–15. Springer, 2010.

[15] Borisov, N., Goldberg, I., Wagner, D., Intercepting mobile communications: the insecurity of 802.11, MOBICOM. pp. 180–189. ACM , 2001.

[16] K. H. M. Wong, Z. Yuan, C. Jiannong, and W. Shengwei,A dynamic user authentication scheme for wireless sensor networks," in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, vol. 1, pp. 318–327, Taichung, Taiwan, June 2006.