Achieving Authentication and Integrity using Elliptic Curve Cryptography Architecture

Ms. Manali Dubal
Research Scholar, University of Pune
SKN College of Engineering
Maharashtra, Pune-41

Ms. Aaradhana Deshmukh, Ph.D.
Scholar, Aalborg University
SKN College of Engineering
Maharashtra, Pune-41

ABSTRACT

Communication security is one of the areas where research is highly required. The data used in communication is very sensitive and needs to be protected and made abstract from intruders of system. This research is all about securing the messages or data that is being communicated among two parties.The recent branch of Network security is Cryptography using Elliptic Curve Architectures which is based on the arithmetic of elliptic curves and discrete logarithmic problems. ECC schemes are public-key based mechanisms that provide encryption, digital signatures and key exchange algorithms. The best known encryption scheme is the Elliptic Curve Integrated Encryption Scheme (ECIES) which is included in IEEE and also in SECG SEC 1 standards. The key establishment protocol is Elliptic Curve MQV, with implicit certificates and symmetric key cryptographic techniques. The research focuses on achieving secrecy using ECIES algorithm for encryption, and authentication using Hashing technique. The hashed plaintext is again encrypted with RSA. At the receiver end, the hashed text is decrypted first. The hash value of the plaintext decrypted is compared with the latter hash. If they are found equal, the integrity can also be assured. The parameters to considered choosing Elliptic Curves are presented in NIST document of recommended elliptic curves.

General Terms

Information and Communication Security

Keywords

Elliptic curve Cryptography, Integrated encryption scheme, information security, encryption-decryption scheme, security in Wireless sensor nodes (MANET's), Message authentication.

1. INTRODUCTION

Main aspects of Cryptography include confidentiality, data integration and authentication. Cryptography was only used for military purposes until modern times. But now a days it is mainly used to secure online states of transactions, ATM and smart cards, that depend on cryptography.

As network communication is used in everyday life, it has become apparent that our privacy is at stake. The key issue for the cryptographic community since starting is the method of distributing the encrypted data to a large set of users, such that only the subset of privileged users can decrypt the data.

Even if the data is received by other users, they should not be able to fetch or decrypt because of non-availability of decryption key. The key is only revealed to the receiver parties through key exchange algorithm. Moreover, the data which is send to the receiver must authenticate the sender so that identity issues are handled during message transmission. Proof of identity or certificates are to be issued by both the parties for authentication.

This paper introduces the method of secure transmission of message through sensor nodes. Although complete security of system is very unfeasible now a days, certain approaches have been defined which would try to achieve the basic security criteria of integrity, authentication and secrecy.

In next section, the elaboration of problem statement and related work is discussed. Section 3 defines the proposed architecture model as well as description explaining each of the modules of the system. Section 4 discusses the expected outcome with expected results. Section 5 concludes the paper and Section 6 describes the papers, journals and thesis referred in the context.

2. RELATED WORK

Mobile Adhoc Networks are very widely used now a days due to the features such as scalability, dynamic infrastructure and intelligent decision making capabilities. To provide security to such networks, vulnerabilities must be first identified and different solutions can be suggested based upon the implantation requirements. The sender of data considers two major factors for transmission: 1. How efficient the transmission is and 2. Secure transmission using lowest possible bandwidth requirements. Counting on these two features, several authors have commented and articled methods to achieve best possible secure transmission. The detailed review can be found below.

2.1 Study of Protocol and Attacks in MANET's

The major challenges for wireless Adhoc networks are: Multicast Routing, Quality of Service, Internetworking and power consumption [1]. The communication in Adhoc networks is through routing and thus any leakage or modification of information would occur only during routing through different nodes [2]. Several routing protocols have been proposed which are table-driven as well as demand-driven [3] [4]. DSDV (Destination Sequenced Distance Vector) – proactive routing protocol, maintains the table for each hop count and sequence number, is vulnerable to wormhole attacks as the colluding nodes may try to send other authenticated nodes the false information, which leads to false communication. Another proactive routing protocol is OLSR (Optimized Link State Routing). Remote nodes may send false information to the communicating nodes which leads the farther nodes to assume they are neighboring nodes and in turn leads to failure of routing protocol. [9] AODV (Adhoc On-demand Distance Vector) is a reactive routing protocol which is using demand-driven approach. The nodes send route request messages (RREQ) to the neighboring nodes to find the path to the destination node. The intermediate nodes in turn send the same messages to neighbors, and determine the path from source to destination by receiving RREP messages – Route Reply Messages [8].

Moreover, the routing protocol must support symmetric as well as asymmetric cryptographic operations. Patroklos G. Argyroudis et. al.[10], proposed an extension to AODV protocol – Secure Adhoc On-Demand Distance Vector (SAODV). This protocol used digital signatures and hashing mechanisms to secure AODV message packets. To have feasible transmission of message, SAODV provides a standard message format.

Type	Length	Hash Function	Max Hop Count
Top Hash			
Signature			
Hash			

Fig. 1: SAODV Protocol Header [10]

The calculation of Signature and Hash can be obtained from section 4. The performance analysis of these routing protocols state that, while considering the worst case of high mobility and high traffic, SAODV protocol provides average end to end delay, Packet Delivery Ratio, Route overhead and Path optimality. Furthermore, it is less prone to attacks as compared to other protocols. Thus in this research the communication is through routing using SAODV protocol.

2.2 Study on various algorithms used for Security purpose

Besides routing, the protocol used for communicating nodes plays most important role during information exchange [6]. The more secure the architecture used is, the more secure the information exchange will be. Even though the colluding nodes or other malicious nodes try to fetch the content during transmission, the algorithm should be such that analysis of information is not possible. Different means of ensuring integrity and confidentiality of data have been proposed. In all modern crypto primitives, the security more or less depends on the security of the cryptographic keys hence the distribution and management of keys has a vital importance [6][10] . As we know, public key cryptography simplifies key management by allowing secure communication by distributing n public key-private key pairs in a network having n nodes whereas the same problem can be solved by distributing $n * (n\text{-}1) \approx n^2$ keys with symmetric key cryptography.

The main research problem to target to is to reduce the number of keys to overcome the limitations of communicating nodes. A brief survey of key distribution mechanisms and alternatives is been proposed by Campete and Yener[11]. Other studies also showed the feasibility of implementing public key algorithms, such as ECC in hardware, RSA in software, over sensor nodes.

The table summarizes the key size of ECC algorithms and comparison of other key sizes. It can be clearly observed that ECC has smaller key size as compared to other systems and this solves the first and foremost issue of key management in wireless networks.

Table 1. Key Sizes in bits and Equivalent Levels

Symmetric	**ECC**	**DH/DSA/RSA**
80	163	1024
128	283	3072
192	409	7680
265	571	15360

Moreover, the execution time of ECC over certain frequency processors, for encryption and decryption can be compared by following table. [10] The hardware of such processors supports the scalar multiplication and other ECC arithmetic operations.

Table 2. Key Sample ECC Exponentiation over GF(P) and RSA Encryption/ Decryption Timings in milliseconds. Here, RSA-1 is for public key operation and RSA-2 is for private key operation

	163 ECC	**192 ECC**	**1024 RSA-1**	**1024 RSA-2**	**2048 RSA-1**	**2048 RSA-2**
Ultra Sparc II 400MHz	**6.1**	**8.7**	**1.7**	**32.1**	**6.1**	**205.5**
Strong ARM 200MHz	**22.9**	**37.7**	**10.8**	**188.7**	**39.1**	**1273.8**

This research focuses on all the issues mentioned above and tries to provide an efficient solution to challenges of Adhoc networks.

3. THE PROPOSED SCHEME

The proposed scheme adopts encryption and decryption using hybrid architecture as shown in Figure 2 and 3.

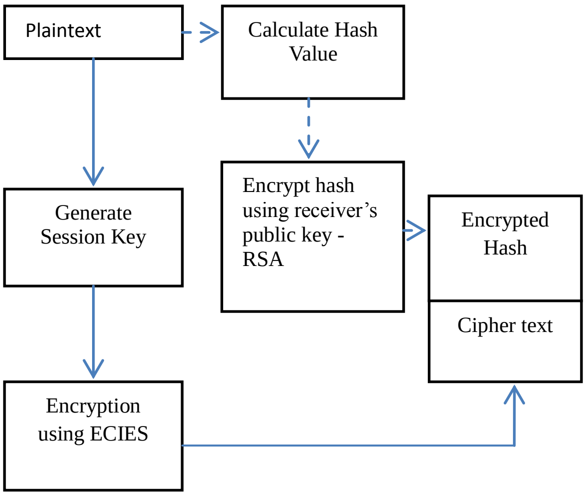

Fig. 2: Encryption Procedure

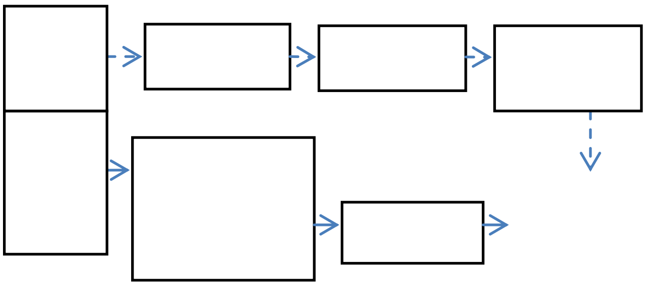

Fig. 3: Decryption Procedure

Elliptic curve cryptography is being used popularly over years due to the fact that it has fundamental and very efficient technological alternatives for building up secure public key cryptosystems. They provide distinct advantages such as smaller key sizes and higher security strength for each bit of the data. The major issue of key storage for Adhoc networks can also be solved using ECC.

As these cryptosystems require fewer amounts of storage and low bandwidth requirements, they are feasible to implement over wireless networks. The security depends on the difficulty of solving discrete logarithmic problem for large prime numbers. The more the problem difficulty is, the better the security is [12][3].

3.1 Introduction to Elliptic Curve Cryptosystems

Elliptic curves have been used to solve a range of problems by mathematicians. The concept was first proposed by Neal Koblitz and Victor Miller to design public-key cryptographic systems.

Definition 3.1 An elliptic curve E over a field F is defined by an equation,

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad \text{(i)}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$, where Δ is the discriminant of E.

Definition 3.2 For a Weierstrass equation as above the following quantities can be defined

$$b_2 = a_1^2 + 4a_2 \qquad \text{(ii)}$$

$$b_4 = 2a_4 + a_1a_3 \qquad \text{(iii)}$$

$$b_6 = a_3^2 + 4a_6 \qquad \text{(iv)}$$

$$b_8 = a_1^2 a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \qquad \text{(v)}$$

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + b_2b_4b_6 \qquad \text{(vi)}$$

Definition 3.3 Let F is a field of characteristic different from 2 or 3. Let E be an elliptic curve defined over F. Then there exists a Weierstrass model for E of the form:

$$y^2 = x^3 + Ax + B \qquad \text{(vii)}$$

where A, B are elements of F and ensure that

$$4A^3 + 27B^2 \neq 0 \qquad \text{(viii)}$$

to avoid degenerate cases.

If the values of x, y, A, and B belong to a field F, it can be said that elliptic curve E is defined over the field F, and is denoted by the set of points:

$$E(F) = \{(x, y) \in F \times F \mid y^2 = x^3 + Ax + B\} \cup \{O\}$$

where A and B are some fixed constants, and O is the point at infinity.

The EC Domain Parameters are 7-tuple : T = (p,a,b,G,n,h), where p is the finite field of the defined curve, a and b are elements of the elliptic curve equation, G is the generator point or the base point which has the property of generating all other points defined by same equation, n is the order of point G and h is the cofactor.

The security of elliptic curve cryptosystem relies on the fact about Discrete Logarithmic Problem. The more the problem is difficult, the better the security is.

3.2 Key Agreement and Management

ECMQV (Elliptic curve Menezes–Qu–Vanstone) is an authenticated key agreement protocol, which is based on Diffie-Hellman scheme. Considering the worst case of active attacks, this algorithm is best suitable for such an environment.

3.3 Encryption using ECIES

Elliptic curve integrated encryption scheme is used to provide semantic security against untrusted third party. This scheme provides safety against adaptive chosen-plaintext and chosen-ciphertext attacks. It provides capabilities for encryption, key exchange and digital signature together. Hence it is called Integrated Encryption Scheme. It is recommended by NIST, SECG, SEC 1 standards due to aforementioned characteristics.

ECIES is the enhancement of ElGamal encryption scheme, designed specifically for Elliptic curve groups. In this project, the suite uses following algorithms:

1. Key agreement ECMQV (as previously specified)
2. MAC – HMAC-SHA-1 with 160 bit keys
3. Symmetric encryption scheme, AES in Cipher block chaining mode (CBC).

After the key agreement protocol has been established, the derived MAC key MAC_{k1} and the message to be transferred m, are given as input to symmetric encryption algorithm, ENC such as AES or Triple-DES (TDES). The sender encrypts the message with symmetric encryption key MAC_{k1} to generate:

$$c = E(MAC_{k1},m) \tag{ix}$$

Then it computes an authentication token d for the ciphertext as an encryption of the ciphertext with MACk1, such that

$$d = MAC(MAC_{k1},E) \tag{x}$$

Implementation of TDES takes more time as compared to AES. The block size of AES is 128, 192 or 256 bits while of TDES is 64bits. Thus the time complexity of processing AES in block cipher mode would be less as compared to TDES. By using integrated encryption scheme, integrity of data that is being communicated is preserved.

Sender Node	Receiver node
1. Generates k_S, session key and computes transient public key $sk_A = k_S * P$ *Req* (ID_A, sk_A) →	2. Receiving first message, - Generates transient public key $sk_B = k_R * P$ - Calculates $s_B = (k_R + \overline{sk_B}\, d_B) \bmod n$ and - $R = hs_B(sk_A + \overline{sk_A}\, Q_A)$; $\overline{sk_B}, \overline{sk_A} \leftarrow$ integer representation of the x-coordinate of sk_B, sk_A, h is elliptic curve domain parameter. - $(k_1, k_2) \leftarrow KDF(x_R)$, where x_R is x-coordinate of R and KDF is key derivation function. - Calculate $t_B = MAC_{k1}(2, ID_B, ID_A, sk_A, sk_B)$ *Rep*(ID_B, sk_B, t_B) ←
3. On receiving second message, - Calculate $s_A = (k_S + \overline{sk_A}\, d_A) \bmod n$ and $R = hs_A(sk_B + \overline{sk_B}\, Q_B)$; - $(k_1, k_2) \leftarrow KDF(x_R)$ - $t = MAC_{k1}(2, ID_B, ID_A, sk_A, sk_B)$ and verify $t = t_B$ - $t_A = MAC_{k1}(3, ID_B, ID_A, sk_A, sk_B)$ *Rep* (t_A) →	On receiving the last message, this node computes $t = MAC_{k1}(3,ID_A,ID_B, sk_A,sk_B)$ and verifies that $t = t_A$

3.4 Calculating Hash of plaintext

For authenticating the sender of message, and vice-versa, hashing technique is used. SHA-1 produces 160-bit of message digest and performs 80 rounds of operation. The input data is divided into 32-bit blocks and left shift is done with variable n. The value of n varies at each operation resulting into new left rotation every time. This value is X-ORed with the round constant of the current iteration.

The plaintext is hashed and encrypted by RSA algorithm for the same key as used for ECIES encryption. As the technique is symmetric encryption, the receiver should decrypt the hash as well as ciphertext using the same key.

On the receiver side, first the hash is decrypted and the ciphertext is decrypted, then the hash of plaintext is computed using SHA-1. The hash values are compared, if they are found equal, the sender of the message is the one it claims to be. Thus authentication can be proved and integrity is also maintained.

4. EXPECTED RESULT ANALYSIS

4.1 Cost for creating session keys

The sender generates two elliptic curve points: 1). which derives the symmetric encryption and the MAC key MACk1. 2). which is used by the receiver to derive the point P. Generation of these two points require two elliptic curve scalar multiplication procedure, which takes *2log(p).* The receiver calculates the point P from the request message and the cost is incurred is *log(p).* As experimented by [6], the cost of multiplication of standard elliptic curve points on Pentium II 400 MHz Platform is:

F_2^{163} (µsec)	F_2^{233} (µsec)	F_2^{283} (µsec)
16.36	27.14	37.95

4.2 Cost for encryption messages

The cost of encrypting messages using ECIES is the cost incurred in encrypting AES in CBC mode, which is certainly less than the cost of calculating keys. As described by [6], the cost of encrypting messages through ECIES on Pentium II 400 MHz Platform is:

Key Size (bits)	Block Size (bits)	Encryption Time (µsec)
128	128	0.863
128	192	1.530
128	256	2.405

5. CONCLUSION

The paper presents the security protocol for securing data between two communicating nodes in mobile adhoc networks. Specifically military applications require most high secure message routing functionality.

The algorithm used for encryption is ECIES which is best known security algorithm for the latest cryptographic attacks. Expected outcome is, the proposed scheme would solve the issues of space in terms of key management in adhoc networks as well as it will provide integrity and authentication for the communicating entities.

6. ACKNOWLEDGMENTS

Author Manali Dubal expresses her sincere gratitude to Prof. Ms. A. A Deshmukh for her support to carry out this research and continuous guidelines for making this paper a fruitful venture.

7. REFERENCES

[1] Xixiang LV, Hui LI, Baocang WANG,“Identity-based key distribution for mobile Ad Hoc networks”, Springer-Verlag Berlin Heidelberg 2011

[2] Kamal Kumar Chauhan, Amit Kumar Singh Sanger, Virendra Singh Kushwah, “Securing On-Demand Source Routing in MANETs”, IEEE- Second International Conference on Computer and Network Technology-2010

[3] Kavitha Ammayappan, V.N.Sastry, Atul Negi, “Cluster based Multihop Security Protocol in MANET using ECC”, TENCON 2008, IEEE Conference.

[4] V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila, “A Survey of the Elliptic Curve Integrated Encryption Scheme”, Journal Of Computer Science And Engineering, Volume 2, Issue 2, August 2010.

[5] Johann Heyszl, Frederic Stumpf, “Efficient One-Pass Entity Authentication based on ECC for Constrained Devices”, 2010 IEEE, 978-1-4244-7812-5.

[6] Miguel Morales-Sandoval and Claudia Feregrino-Uribe, “A Hardware Architecture for Elliptic Curve Cryptography and Lossless Data Compression”, International Conference on Electronics, Communications and Computers (IEEE-CONIELECOMP 2005)

[7] V. Gayoso Martinez, L. Hern´andez Encinas, and C. S´anchez ´ Avila, “Java Card implementation of the Elliptic Curve Integrated Encryption Scheme using prime and binary finite fields”, Computational Intelligence in Security for Information Systems, Springer, 2011.

[8] Shadi S. Azoum, “Secure Real-Time Conversations”, Thesis, Florida State University, Spring 2008.

[9] Kavitha Ammayappan, V.N.Sastry, Atul Negi , “Authentication And Dynamic Key Management Protocol Based On Certified Tokens For Manets”, IEEE-Global Mobile Congress 2009.

[10] Patroklos G. Argyroudis et. al, “Secure Routing for Mobile Ad Hoc Networks”, IEEE Communications Surveys, 2005

[11] Campete, S.A., Yener, “Combinatorial design of key distribution mechanisms for wireless sensor networks”, IEEE/ACM Transaction Network, 2008

[12] Chiang, Chien-Wen, “A new scheme of key distribution using implicit security in wireless sensor networks”, IEEE-Advanced Communication Technology (ICACT 2010)

8. AUTHOR’S BIOGRAPHIES:

Ms. Manali Dubal received her B Tech degree in Information Technology from University of Saurashtra in 2010. She is currently pursuing Masters in Computer Engineering from the University of Pune, India. From 2011 till date, she is serving as Professor at Gujarat Technological University, Atmiya Institute of Technology & Science, Rajkot, India. She has published about 4 journal and conference papers in ACM, IEEE as well as AIRCCE. Her research interest covers information and communication security. She has been on the reviewer as well as editorial board for many national international conferences and journals. She is a student member of ACM, member CSI, CSTA, IAENG. E-mail: manali.dubal@gmail.com

Ms. Aaradhana Deshmukh received her B.E degree in Computer Science & Engineering, VIT, Pune, and M.E in Computer Engineeering from PICT, Pune, University of Pune. She has also obtained various degrees like A.M.I.E. Computer Engineering, M.A. (Economics) from Pune University. She is having 10 years experience in Teaching Profession and 2 ½ years R & D experience in various institutes under Pune University. She has published more than 50 papers, 8 in International Journals like ACM, IJCSI, ICFCA,IJCA etc, 16 in International Conferences like IEEE etc., 5 in National Conferences, 4 in symposiums . She has received Gold Medal at International level Paper Presentation on “Neural Network” as well as one more for “UWB Technology based adhoc network”, in International Conferences.

She is recipient of ‘Distinguished Alumni Award’ in 2011 from Inst. Of Engineers [India] , Gunawant Nagrik Puraskar for the year 2004 – 2005, ‘Anushka Purskar’ from Pimpri Chinchwad Municipal Corporation, and also won many Firodiya awards . She is also member of Zep, CSI, Pune. E-mail: aadeshmukhskn@gmail.com