An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks

Ms.P.G.Rajeswari
Assistant Professor, Department of Mathematics
V.L.B.Janakjammal College of Engineering and Technology, Coimbatore 42.

Dr.K.Thilagavathi
Reader
Department of Mathematics
Kongunadu Arts And Science College
Coimbatore 29.

Summary
Mobile Networks offer unrestricted mobility devoid of any underlying infrastructure. Typically, mobile networks are deployed in un-trusted environments. Such networks in this day and age have to keep privacy and security of data as a top concern, because eaves dropping peaks here. The root cause behind such eavesdropping is the un-authenticated access of base station on nodes. The eventual outcome is the menace of insecure environment, information misuse, and so on. Cryptosystem is an important technique to identify the authenticity in order to protect the confidential and sensitive data in mobile networks. This paper proposes a simple and efficient authentication protocol for the establishment of secure communication between base station and nodes in mobile networks. The protocol proposed, here, is new one for authentication scheme, having simplicity and efficacy. The protocol is designed by employing a most familiar public-key cryptographic scheme, elliptic curve cryptography and then it is dedicated to mobile networks for authentication of base station. Usage of this protocol in mobile networks will allow only the authorized base station to access the node and hence it will deny the information to eavesdroppers when they try to hack or misuse the node.

Keywords:
Mobile Networks, Authentication Protocol, Pubic-key cryptography, Elliptic curves Elliptic Curve Cryptography (ECC), Key pair.

1. Introduction

In today's world, information security is crucial, which is necessitated by the profitable and legal trading, confidentiality, integrity and non-reputability of the associated information. Along with the arrival of mobile networks, new security requirements come up because of the shortage in physical protection means similar to the traditional fixed-topology, static user networks. Illegal access (fraud), eavesdropping are some of the security concerns in mobile networks. Recently, new security questions are prompted by the rapid progress in wireless mobile networks. Secure communication, an important aspect of any networking environment, is especially a significant challenge in mobile networks. In the view of the fact that the communication channel employed in mobile networks is air, there are lots of possibilities for information snoop from nodes by un-authorized base stations that are pretending as the valid one. It is necessary to provide certain security measures, e.g., confidentiality, authenticity, and no traceability so as to have reliable proper security over the mobile networks [16]. A secure communication system contains preferred properties which may include any or all of the following [2]:

- **Confidentiality**: The contents of the encoded data can be extracted in part or whole only by an authorized recipient.
- **Integrity:** In case the message has been altered during transmission, the recipient should be able to establish it.
- **Authentication**: It is necessary that the recipient identifies the sender and verifies that the message was actually sent by the purported sender.
- **Non-Repudiation**: If the sender actually sends the message, it should not be able to deny the sending of the message.
- **Anti-replay**: The message should not be permitted to be sent to multiple recipients, devoid of the sender's knowledge.
- **Proof of Delivery**: The sender should posses the ability to prove that the message was received by the recipient.

Authentication can be said as any process by which one can verify that someone is who they claim they are. The ability of a node to ensure the identity of the peer node it is communicating with is facilitated by the security primitive known as authentication. It is not the best strategy for protecting availability, integrity and confidentiality when we grant resources to, obey an order from, or send confidential information to a principal of whose identity we are unsure [5].Privacy protection is supported by authentication which ensures that entities verify and validate one another before disclosing any secret information. Additionally, authentication allows access to services and infrastructure by authorized entities only, while denying unauthorized entities access to sensitive data, thereby supporting confidentiality and access control. While transmitting confidential data in case of mobile networks, it is vital that the receiver that receives the

Manuscript received February 5, 2009
Manuscript revised February 20, 2009

information is the one it is meant for. For instance, a base station can gain unauthorized access to resources and sensitive information by masquerading as another base station.

Consequently, in most applications where security matters, it is necessary to attain authenticity, which is an essential prerequisite achieved by employing cryptographic systems. All the above-mentioned requirements are satisfied by the integrated cryptographic systems [3].The performance of the protocol following the cryptographic schemes is good, especially public-key systems. The authentication protocol using RSA algorithm belongs to the category of public-key cryptography. Owing to the fact that it is on the basis of the creation of mathematical puzzles that are difficult to solve without certain knowledge about how they were created, it performs well. However, for providing adequate security the RSA keys should be at least 1024 bits long. Recently, elliptic curve cryptography is gaining popularity in cryptosystems because of its enhanced security with lesser key size. Elliptic curve cryptographic schemes are public-key mechanisms, identical to RSA schemes in functionality. Elliptic curve systems aid in obtaining the desired security level with considerably smaller keys than that of the corresponding RSA schemes. For instance, a 164-bit elliptic curve key is considered to offer identical level of security as a 1024-bit RSA key. Speed and efficient use of power, bandwidth, and storage are some of the significant merits of utilizing smaller keys [27].

In our paper, we propose an efficient authentication protocol based on Elliptic curve Cryptography, a public key system that offers reasonable security with lesser key length when compared to RSA algorithms. A class of finite groups is provided by the mathematical theory of elliptic curves that have proven quite suitable for cryptographic use. Also some thriving features that made elliptic curve cryptography [20] more suitable for authentication is as follows

- For a given key size, ECC offers considerably greater security.
- For a given level of security, much more compact implementations are also made possible by the smaller key size, which means faster cryptographic operations, running on smaller chips or more compact software. This also means less heat production and less power consumption, all of which is of particular advantage in constrained devices, but of some advantage anywhere.
- Extremely efficient, compact hardware implementations are available for ECC exponentiation operations, in which potential reductions in implementation footprint even beyond those due to the smaller key length alone are offered.

All these factors show the elliptic curve cryptography is fit for authentication and hence on the basis of the mathematical theories of elliptic curve, we designed a new protocol for base station authentication in mobile networks. The rest of the paper is organized as follows. In section 2, the concentration is on the definitions of authentication, its categories and some systems that are suitable for achieving authentication in networks. Section 3 focuses on the heart of our protocol, elliptic curve cryptography, its fundamentals and mathematical theories. The steps of the protocol we have proposed, key pair generation procedures the authentication procedures and are construed with required visuals in section 4 and also the code verification is developed in this section. Section 5 holds the experimental results obtained in response to the protocol. Some past works done for defining protocol for authentication and the usage elliptic curve cryptography in different other fields occupy as related works in Section 6 and the conclusion finalizes the authentication protocol based elliptic curve cryptography is simple and efficient.

2. Authentication

Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true [1]. In general, authentication means the existence of some method for ensuring that the entity to which you are talking to is who it claims to be, known as authentication of the channel end point. Typically it is necessary to authenticate yourself to the service so that the service can be sure that you are you, not someone else who is pretending to be you, which is the authentication of the message originator [8]. There are several requirements for authentication in which protection against replay attacks; confidentiality, resistance against man-in-the-middle attacks etc. are included. Any authentication scheme employed includes all the above requirements. The basic textbooks about computer security provide more information about authentication methods and threats that they may have [6] [7].

2.1. Categories of Authentication

The term strong user authentication is used from time to time, in which any authentication process that increases the likelihood that an identity of base station will be verified correctly is described, which can be accomplished with long complicated passwords or combining two or more authentication factors.

Generally, three authentication factors [4] are distinguished:

- Knowledge factor – information known by the user has to be presented, for instance, a password.
- Possession factor – something possessed by the user has to be presented, for example- tokens or keys.
- Being factor – Contrasting to the former two factors, something of user has to be presented, for instance- physical parameters.

The use of a password is the most common case. As passwords are typically short and easy to break, it is not really a good choice. There are more secure methods, in which the use of public key cryptography, challenge-response schemes, symmetric encryption, etc is included.

The effectiveness of any authentication protocol mainly depends on the method involved in the generation of secured key pair. Secured key pair refers to the maximum complexity in identification or hacking them. In our protocol, we are applying public key cryptography in the authentication scheme for key generation. Among the different public key cryptographic schemes, Elliptic curve cryptography shines because of its thriving feature of generating key that could not be easily hacked.

3. Elliptic Curve Cryptography

Conventional public key cryptosystems (RSA, DSA, and DH) [14] are being replaced by the budding technology of Elliptic Curve Cryptography (ECC). The issue of implementing public key cryptography on mobile computing devices [10] has been resolved with the aid of ECC. Elliptic Curve Cryptography (ECC) has two significant merits: one is that it is well investigated and thus remarkably secure and the other is that it demands a comparatively shorter length that the other asymmetric systems [9]. Faster computations and lower power consumption besides memory and bandwidth savings occur as a result of these beneficial features of the ECC.

We begin with the definition of fundamentals of elliptic curve cryptography and its mathematical formulations. The authors of [19, 18] have discussed in detail about the mathematical background of the elliptic curve cryptography.

3.1. Fundamentals of Elliptic Curve Cryptography

Some fundamentals of elliptic curve cryptography that is essential to understand the mathematical descriptions of elliptic curve used in the cryptographic scheme is discussed below

- **Scalar:** Any element that is a constituent of either $GF(p)$ or $GF(2^k)$ is termed a scalar. Lower case letter are utilized to denote scalars.
- **Scalar addition:** A new scalar can be obtained as a result of the addition of two or more scalars. Common integer addition modulo p is the addition in case of $GF(p)$. This is comparable to polynomial addition modulo an irreducible polynomial of degree k, generating the field $GF(2^k)$ when $GF(p)$ is utilized. The scalar addition of r and s producing *e* is given by $e = r + s$.
- **Scalar Multiplication:** A new scalar can be obtained by the multiplication of two or more scalars. Common integer multiplication modulo p is the multiplication in case of $GF(p)$. This is comparable to polynomial multiplication modulo an irreducible polynomial of degree k, generating the field $GF(2^k)$. The scalar multiplication of r and s producing *e* is given by $e = r \cdot s$.
- **Scalar Inversion:** a^{-1}, the denotation of multiplicative inverse of any constituent element of $GF(p)$ or $GF(2^k)$ has the property $a.a^{-1} = 1$. The Fermat's method or the extended Euclidean algorithm aid in its computation.
- **Point:** A point may be defined as an ordered pair of scalars conforming to the elliptic curve equation. These elements are denoted by capital letter such as P_1, P_2, etc. An alternative notation for a point P_1 is $P_1 = (x, y)$ where both x and y belong to the field. For obvious reasons the coordinates x and y of point P_1 are denoted as $P_1 \cdot x$ or $P_1 \cdot y$, respectively.
- **Point Addition:** It is possible to obtain a third point R on the curve given two points P and Q with the aid of a set of rules. Such a possibility is termed elliptic curve point addition. The symbol ` + ' represents the elliptic curve addition $P_3 = P_1 + P_2$. Point addition is not to be confused with scalar addition.
- **Point Multiplication:** $e \times P_1$ denotes the multiplication of an elliptic curve point P by an integer *e.* This is analogous to the addition of P_1 to itself e times and this results in another point on the curve.

- **Elliptic Curve Group:** When the above discussed point addition operation is considered as a group operation, an additive group that consists of the set of the solutions of the elliptic curve equation and a special point called point-at-infinity, is formed.

3.2. The Mathematical Theory of Elliptic Curves

A class of finite groups that have been established quite appropriate for cryptographic use is put forth by the theory. Neal Koblitz [12] and Victor S. Miller [13] independently recommended the utilization of elliptic curves in cryptography in 1985.

Two kinds of finite fields namely the fields of odd characteristic (Fp , where p > 3 is a large prime number) and fields of characteristic two (F_{2^m}) serve as the basis for defining the elliptic curves utilized in cryptography. When the features are of futile significance, they are denoted as F_q , where $q = p$ or $q = 2m$.

A locus of points in the elliptic curve whose coordinates conform with a particular cubic equation along with the point at infinity O (the point at which the locus in the projective plane intersects the line at infinity) is known as an elliptic curve.

The equation of $E(F_p)$ for the characteristic p > 3 can be defined as

$$y^2 = x^3 + ax + b \tag{1}$$

Where $a \in F_p$ and $b \in F_p$ are constants such that $4a^3 + 27b^2 \neq 0$. In the binary case the defining equation of can be $E(F_{2^m})$ written:

$$y^2 + xy = x^3 + ax^2 + b \tag{2}$$

Where $a \in F_2$ and $b \in F_{2^m}$ are constants and $b \neq 0$.

A collection of points can be formed with the aid of a chord-and-tangent rule (extended addition) in an elliptic curve E defined over the field K as denoted in figure 1.

Using basic coordinate geometry and given two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, one constructs arithmetic to compute the point $P_3 = (x_3, y_3) = P_1 + P_2$ as follows:

$$x_3 = \lambda^2 - x_1 - x_2 \tag{3}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \tag{4}$$

Where

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1), & if \quad p_1 \neq p_2 \\ (3x_1^{\,2} + a)/(2y_1), & \text{otherwise} \end{cases} \tag{5}$$

The addition of two EC points is illustrated [15] in the figure1.

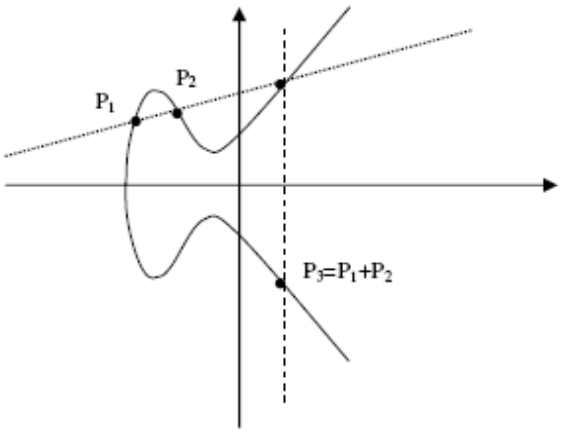

Fig. 1 Addition of two elliptic curve points

Let P_1 and P_2 be two distinct points that are a part of the set and let them intersect the elliptic curve in a straight line then the straight line with the curve will bear a third intersection. The sum of P_1 and P_2 represented as P_3 is obtained the reflection on the x axis of the third intersection. An Abelian group [17] is created with the set of points defined by the extended addition extended by the point ∞.

4. Authentication Protocol Based on ECC

In mobile networks, the base station may request the node for information. Such requesting station should be an authorized one. However some times it would be an adversary. So, it is very essential to check for the authorization of the base station. Otherwise the pretending one can gain unauthorized access to resources and sensitive information from nodes. Thus the network is forced to operate in an insecure environment. The proposed protocol verifies the authentication of the base station very effectively and paves the way for a secure network. Since the protocol uses Elliptic curve cryptography, a very little key is enough for obtaining the required security. This reduces the bandwidth allocation for key and so the security constraints will not affect the bandwidth by any means, an additional advantage over other schemes.

4.1. Protocol Flow

Sundry signals flow between the node and base station for the verification of authentication of the base station. In response to the authentication verification, the information may be passed or a warning may be given to the base station for its hacking intention. A schematic view of the proposed protocol is explained by the following signal flow diagram.

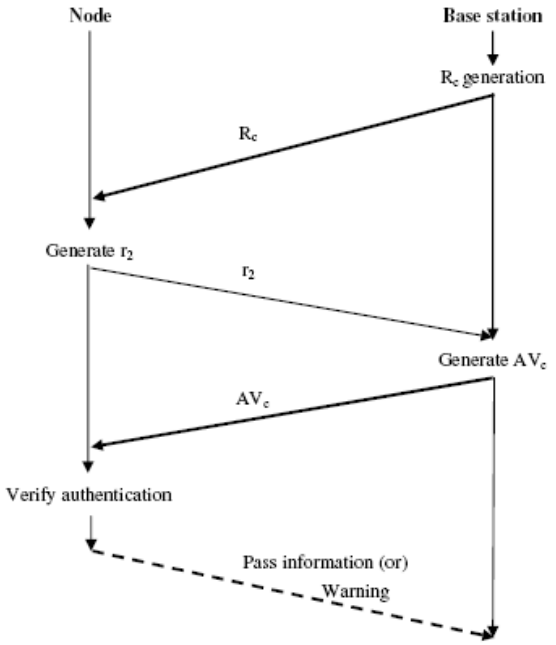

Fig. 2 Protocol Flow for Authentication

The authentication can be determined just in three steps of message transformation. The message transfer is initiated by the requesting base station by using requesting code R_C. Then the node response for the request and then it verifies the authentication of the requested base station.

The initial process that needs to demonstrate the protocol is key pair generation influencing wholly by the elliptic curve cryptography. After key pair generation, the base station obtains a private key and public key and then it will be subjected for the authentication procedure.

4.2. Key Pair Generation

Key pair generation is one of the responsibilities of the elliptic curve cryptography and it is the major area in which the elliptic curve participates in our work. Key pair as mentioned here is nothing but a combination of private key and a public key. The mathematical derivation for the generation of key pair using the same is as follows.

In the remainder of this article we will only focus on elliptic curves defined over F_p, where p is a "large" prime number. Field elements will be naturally represented as integers in the range $0,1,\cdots,p-1,$ with the usual arithmetic modulo- p.

Let F_p be the prime finite field. It is a set contributed by integers modulo p, where p is the random prime number.

An elliptic curve E over F_p is defined by an equation of the form

$$y^2 = x^3 + ax + b \tag{6}$$

Where $a, b \in F_p$ should satisfy,

$$4a^3 + 27b^3 \not\equiv 0(\text{mod } p) \tag{7}$$

The point at infinity, denoted by ∞, is also said to be on the curve. $E(F_p)$ denotes the set of all the points on the Elliptical curve E.

Let P be a point in $E(F_p)$, and suppose that B has prime order m. Then the cyclic subgroup of $E(F_p)$ generated by B is

$$< B >= \{\infty, B, 2B, 3B, ...(m-1)B\} \tag{8}$$

The prime p, the equation of the elliptic curve E, and the point B and its order m, are the public domain parameters. A private key is an integer K_s that is selected uniformly at random from the interval $[1, m-1]$, and the corresponding public key is given by

$$K_p = K_s B \tag{9}$$

Eventually, the protocols factors B, K_p and K_s are found out with the help of the properties of Elliptical curve.

K_p, the public key and K_s, the private key belongs to the base station and B is the generating point from the points of elliptical curve.

4.3. Authentication Procedure

The step-by-step procedure for base station authentication is as follows.

Initially, the base station that needs to access the node will generate a random number r_1. Then it will calculate the requesting code R_c as follows

$$R_c = r_1 * B \quad (10)$$

Consequently the value R_c will be sent to node as request.

Now, the verification of the authentication of the corresponding base station begins. In order to achieve that, the node will generate a random number r_2 and send it to base station.

The base station will generate authentication-verifying code AV_c as a response. AV_c is derived as follows,

$$AV_c = r_1 + (r_2 * K_s) \quad (11)$$

This AV_c will be sent to the node for its authentication verification.

The code verification is given below

$$(AV_c * B) - (r_2 * K_p) = R_c \quad (12)$$

If the above condition is satisfied, the node will come for a conclusion that the base station is a valid one and not an eavesdropper. The condition will be satisfied only if the private key, public key and the generating point are same. Otherwise the condition will be false. This false result happens when a stranger tries to make contact with the node.

After checking for authentication of the base station the node will start its message transformation. If the base station is found to be an eavesdropper, a warning about its un- authentication will be given to the corresponding base station.

The base station authentication procedure proposed in our protocol is strictly followed by the node and is succinctly displayed in the following flowchart.

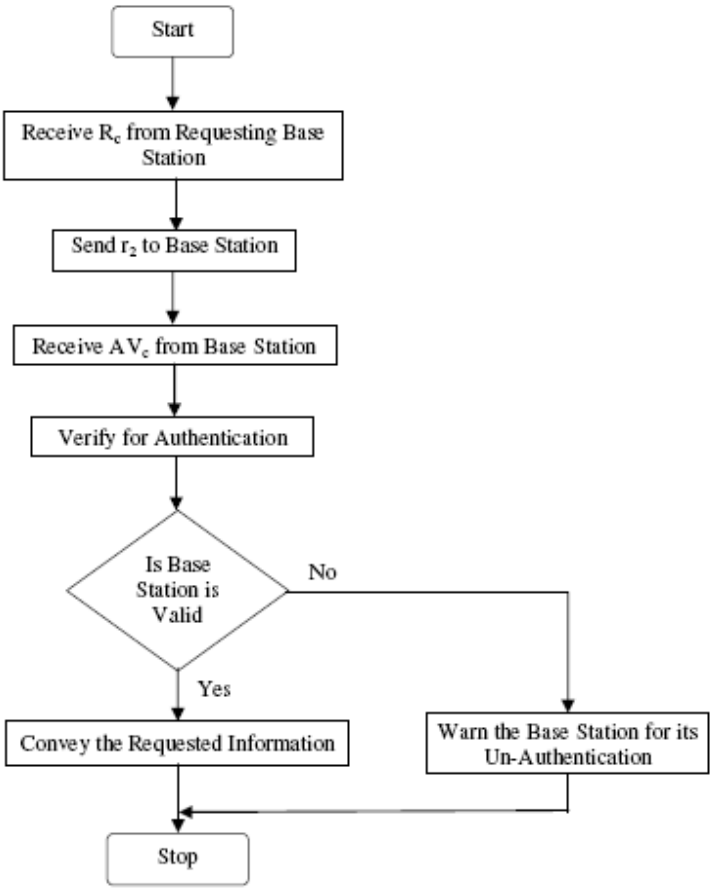

Fig. 3 Flowchart of Authentication Procedure

In fact, the flowchart illustrated above says the authentication procedure from the point of node that is going to verify the authentication of base station. The node

sends the random number r_2 just after the reception of R_c. The authentication of the base station is verified with the aid of the AV_c received from the base station. After the verification of authentication of the base station the node then responses either by conveying the information if the base station is valid or by giving a warning signal if the base station is a quacking one.

4.4. Development of the Verification Code

In this sub-section the verification code for the authentication protocol is developed in step-by-step manner. Let us take the random number r_1 for initialization of the determination of the equation that is doing authentication verification.

$$r_1 = r_1 \tag{13}$$

Multiply the Basic point of the elliptic curve ' B 'on the sides.

$$r_1 * B = r_1 * B \tag{14}$$

Add $r_2 * K_p$ on both sides of equation (14)

$$(r_1 * B) + (r_2 * K_p) = (r_1 * B) + (r_2 * K_p)$$

$$(r_1 * B) + (r_2 * K_p) - (r_2 * K_p) = (r_1 * B)$$

$$B * \left(r_1 + r_2 * \frac{K_p}{B} \right) - (r_2 * K_p) = (r_1 * B) \tag{15}$$

From the equation (9), it can be written as

$$K_s = \frac{K_p}{B} \tag{16}$$

Applying the equation (16) in equation (15) leads to

$$B * \left(r_1 + (r_2 * K_s)\right) - (r_2 * K_p) = (r_1 * B) \tag{17}$$

But, from equation (11) we know that,

$$AV_c = r_1 + (r_2 * K_s)$$

Hence equation (17) takes the form

$$B\,AV_c - (r_2 * K_p) = (r_1 * B) \tag{18}$$

Referring the equation (10), the term $r_1 * B = R_c$ is replaced in the equation (18)

$$(B * AV_c) - (r_2 * K_p) = R_c \tag{19}$$

It is clear that the equation (19) will not get balanced if any invalid base station tries to access by using its own key i.e. private key. This is the proof and base for the proposed authentication protocol that the protocol is having the robustness to distinguish the authorized and un-authorized base station.

5. Experimental Results

For the implementation of our protocol we assign the base station as server and the node as client and java is used for implementing the protocol. We used Sockets for client Server Communication. The server base station is meant to receive the information and the client node is meant to transmit the information to a valid server base station. Each node and server base station is running on its own I.P. addresses. As stated earlier, there are lots of possibilities for hacking the information by adversary server base station, our protocol at the client node is implemented in java and hence it verifies whether the server base station is authorized or an un-authorized one.

When any of the invalid base station tries to access the node, the node will offer a comment as a warning against the un-authorization of the base station. The results and the necessary parametric values needed to visualize the performance of the protocol are tabulated in the Table 1. The protocol is verified for its response by subjecting some un-authorized base stations and authorized base stations to access the node.

Table 1: Results obtained from implementation of Authentication protocol

S.No	Prime no. for finite field P	Basic point B	Secret key K_s	Public key K_p	Ecc Parameters of Accessing Base station			Requesting code R_c	Authentication verifying code AV_c	Verification code $(AV_c.B)-(r_2K_p)$	Is verification code equals R_c	Comment
					B	K_s	K_p					
1	71	(18, 5)	20	(360,100)	(18,5)	20	(360, 100)	(7016455728, 1949015480)	40035669576	(7016455728, 1949015480)	yes	Authorized Base Station
2	113	(0, 3)	9	(0,27)	(0,3)	9	(0,27)	(0 , 1905961332)	13193506255	(0 , 1905961332)	yes	Authorized Base Station
3	37	(33, 3)	35	(1155,105)	(33,3)	35	(1155, 105	(45812721537, 4164792867)	26803734684	(45812721537, 4164792867)	yes	Authorized Base Station
4	13	(4, 3)	9	(36,27)	(4, 3)	9	(36,27)	(4896012764, 3672009573)	9242060585	(4896012764, 3672009573)	yes	Authorized Base Station
5	73	(57,25)	69	(3933,1725)	(9,7)	6	(54,42)	(69839282490, 30631264250)	92614920914	(762011937522, 592675951406)	No	Un Authorized Base Station
6	11	(7,1)	2	(14, 2)	(7,1)	2	(14,2)	(6619358529, 945622647)	2995815513	(6619358529, 945622647)	yes	Authorized Base Station
7	61	(47, 5)	3	(141,15)	(47,5)	3	(141, 15)	(79796020255, 8488938325)	3787059260	(79796020255, 8488938325)	yes	Authorized Base Station
8	79	(75,30)	58	(4350,1740)	(34,33)	31	(1054, 1023)	(133328914650, 53331565860)	90293126854	(1461427691940, 1418444524530)	No	Un Authorized Base Station
9	47	(20,33)	5	(100,165)	(20,33)	5	(100, 165)	(18340554980, 30261915717)	10669553099	(18340554980, 30261915717)	yes	Authorized Base Station
10	53	(47,10)	30	(1410,300)	(20,33)	5	(100, 165)	(42729150920,70503099018)	7131349846	(-1073386185838, -228380039540)	No	Un Authorized Base Station

As applied when an authorized server base station having its private key '20' and public key (360, 100) wants information from the node, the node checks whether the verifying code equals the requesting code R_c. In our set both the values are (7016455728, 1949015480) and hence they are equal. Thus the comment from the node is "Authorized Base Station". Likely, when an un-authorized base station having its private key '6' and public key (54, 42) tries to access the same node, the verifying code (762011937522, 592675951406) differs from the Requesting code R_c and hence the comment is "Un-Authorized Base Station". From the implementation results, it is very proven that the elliptic curve cryptography based authentication protocol is robust in identifying un-authorized base station.

6. Related Works

A semi-fragile framework aiming at extending public key signature scheme from message level to content level was presented by Qibin Sun et al. [21]. The semi-fragile image authentication watermarking framework combines ECC (error correction coding) and PKI (public key infrastructure) security. By using ECC, they have provided a mechanism allowing minor variations of content features caused by acceptable manipulations (such as lossy compression or watermarking). They also developed a novel approach combining local block-based signatures and a global signature. Local block-based signatures can be used to detect locations of attacks in specific blocks and global signature uses cryptographic hashing and PKI to ensure the global authentication of the whole image.

Dawit Getachew et al. [22] have proposed the elliptic curve based authentication protocol, the CM (Context Management) application was used to manage mutual authentication during initial contact, and subsequent CPDLC (Controller-Pilot Data Link Communications) application messages were authenticated using ATN (Aeronautical Telecommunication Network) keyed message authentication code scheme. The protocol depends on the security of the elliptic curve primitives (e.g. key generation, signature generation and signature verification).The protocol would be of great value to ATN data link security protocol designer, verifier and implementer for other ATN air/ground applications.

Vipul Gupta et al. [23] have offered Elliptic Curve Cryptography (ECC) as a suitable alternative and described the integration of ECC technology into several key components of the Web's security infrastructure. The experiments showed the significant performance benefits from using ECC in secure web transactions. Due to its computational efficiency, ECC can be used in constrained environments where traditional public-key mechanisms were simply impractical.

The true impact of any public-key cryptosystem can only be evaluated in the context of a security protocol. Vipul Gupta et al. [24] have presented a first estimate of the performance improvements that can be expected in SSL (Secure Socket Layer), the dominant security protocol on the Web today, by adding ECC (Elliptic Curve Cryptography) support.

Vipul Gupta et al. [14] have studied the performance impact of using ECC (Elliptic Curve Cryptography) with Secure Sockets Layer (SSL), the dominant Internet security protocol. They benchmark the Apache web server with an ECC-enhanced version of OpenSSL under a variety of conditions. The results showed that an Apache web server can be handled 11%-31% more HTTPS requests per second when using ECC rather than RSA at short-term security levels. At security levels necessary to protect data beyond 2010, the use of ECC over RSA improves server performance by 110%-279% under realistic workloads.

Aytunc Durlanik et al. [25] have proposed an approach for secure SIP (Session Initiation Protocol) authentication by using a public key exchange mechanism using ECC (Elliptic Curve Cryptography). Total execution times and memory requirements of proposed scheme have been improved in comparison with non-elliptic approaches by adopting elliptic-based key exchange mechanism.

V. Vijayalakshmi et al. [26] have proposed an authentication technique which makes use of Elliptic Curve Cryptography (ECC) along with the TOA positioning scheme was implemented to solve the problem of insecurity in sensor networks. ECC got excellent enhanced features which include smaller key size, lesser bandwidth, higher computational capability and lesser hardware. The technique was compared for its performance with Rivest-Shamir-Adelman (RSA) and Mean Power with Rivest-Shamir-Adelman (MPRSA). The simulation results clearly indicated that ECC was well suited for secure localization in sensor networks as it satisfies the constraints of the sensor networks which include minimum bandwidth, power, energy and computational speed.

7. Conclusion

The protocol designed here by the deployment of the elliptical curve cryptography performs well against the eavesdropping of information by any un-authorized base stations. Since it is widely known that the mobile networks are one of the most sensitive areas for information hacking, the simple but effective protocol is a boon in preventing such undesirable hack of information. The implementation of our protocol in java establishes well with its job against access of information. Thus the proposed system aids in achieving secure communication in mobile networks with simple steps and reduced computational complexity.

References

[1] Authentication from http://en.wikipedia.org/wiki/ Authentication
[2] Scott A Vanstone P. Van Oorschot, Alfred J Menezes. Handbook of Applied Cryptography. CRC Press, 1996.
[3] Vivek Kapoor, Vivek Kapoor, Ramesh Singh, " Elliptic Curve Cryptography", ACM Ubiquity, Volume 9, Issue 20, May 20 – 26, 2008
[4] Boertien, N., Middelkoop, E.M., "Authentication in mobile applications", Enschede: Telematica Instituut, 2001.
[5] A.O. Salako. Authentication in Ad hoc Networking, In Proceedings of London Communications Symposium 2002, 2002
[6] Schneier, B., Applied Cryptography, 2nd edition, 1996.
[7] Aboda, B. & Arkko, J. & Harrington, D., Introduction to Accounting Management, Internet draft (work in progress), January 2000. http://www.ietf.org/internet-drafts/draft-ietf-aaa-acct-00.txt
[8] Sami Levijoki, "Authentication, Authorization and Accounting in Ad Hoc networks, May 2000, http://www.tml.tkk.fi/Opinnot/Tik110.551/2000/papers/authentication/aaa.htm
[9] Leif Uhsadel, Axel Poschmann, and Christof Paar, "An Efficient General Purpose Elliptic Curve Cryptography Module for Ubiquitous Sensor Networks "Software Performance Enhancement for Encryption and Decryption (SPEED 2007), 2007.
[10] Manuel Barbosa, Andrew Moss, Dan Page, "Compiler Assisted Elliptic Curve Cryptography", OTM Conferences (2), p.p. 1785-1802,2007
[11] Elliptic curve cryptography from http://en.wikipedia.org /wiki/Elliptic_Curve_Cryptography
[12] N. Koblitz, Elliptic curve cryptosystems, in Mathematics of Computation 48, pp. 203-209, 1987.
[13] V. Miller, Use of elliptic curves in cryptography, CRYPTO 85, 1985.
[14] V. Gupta and D. Stebila and S. Fung, "Speeding Up Secure Web Transactions Using Elliptic Curve Cryptgraphy," 11th Network and Systems Security Symposium, pp. 231--239, 2004.
[15] P.H. Roberts and R.N. Zobel1 , "An Elliptic curve Cryptographic System Design Architecture with application to distributed simulation" from http://ducati.doc.ntu.ac.uk/ uksim/uksim'04/Papers/Zobel-%2004-24/paper04-24%20 CR.pdf

[16] V. K. Garg and J. E. Wilkis. Wireless and Personal communications Systems. Upper Saddle River, NJ: Prentice-Hall, 1996.
[17] L. Uhsadel, A. Poschmann, and C. Paar, "An Efficient General Purpose Elliptic Curve Cryptography," In ECRYPT Workshop, SPEED - Software Performance Enhancement for Encryption and Decryption 2007, pp. 95-104, 2007.
[18] N. Koblitz. A Course in Number Theory and Cryptography. New York, NY: Springer-Verlag, Second edition, 1994.
[19] J. Menezes. Elliptic Curve Public Key Cryptosystems. Boston, MA: Kluwer Academic Publishers, 1993.
[20] Introduction from http://www.deviceforge.com/articles/ AT4234154468.html
[21] Qibin Sun; Shih-Fu Chang; Maeno, K.; Suto, M.,"A new semi-fragile image authentication framework combining ECC and PKI infrastructures", in proceedings of IEEE International Symposium on Circuits and Systems, vol.2, pp: 440-443, 2002.
[22] Dawit Getachew, James H. Griner Jr., "An Elliptic Curve Based Authentication Protocol for Controller-Pilot Data Link Communications", ICNS Conference & Workshop, 2005.
[23] Vipul Gupta, Douglas Stebila, and Sheueling Chang. “Integrating elliptic curve cryptography into the web’s security infrastructure”. In Proc. 13th International World Wide Web Conference on Alternate Track Papers and Posters, pp. 402–403. ACM Press, 2004.
[24] V. Gupta, S. Gupta, S. Chang, and D. Stebila, "Performance analysis of elliptic curve cryptography for ssl," in WiSE '02: Proceedings of the 1st ACM workshop on Wireless security, New York, NY, USA: ACM, pp. 87-94, 2002.
[25] Aytunc Durlanik, and Ibrahim Sogukpinar, "SIP Authentication Scheme using ECDH”, Proceedings of World Academy of Science, Engineering and Technology, volume 8, ISSN 1307-6884, October 2005
[26] V. Vijayalakshmi and Dr. T.G. Palanivelu ,"Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks", IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.6, June 2008.
[27] Introduction from http://searchsecurity.techtarget.com /sDefinition/0,,sid14_gci784941,00.html

P.G. Rajeswari is Assistant Professor, Department of Mathematics in VLB Janakiammal College of Engineering & Technology, Coimbatore, India. She teaches Engineering Mathematics and Applied Mathematics for both under graduate and post graduate Engineering students. At present she is persuing her Ph.D. program in Elliptic curve cryptography. She has authored a book “Engineering Mathematics-I” for 1st year B.E/ B.Tech students. Her research area of interest includes graph theory and cryptography and Network Security.

Dr. K. Thilagavathi is Reader, Department of Mathematics, Kongunadu Arts & Science College Coimbatore, India. She has authored 20 International Journals and 17 TextBooks for Engineering & Arts College students. She is the principal investigator for 2 UGC projects. She has guided 12 M.Phil students and 1 Ph.D. student. Her research areas of interest includes graph theory and cryptography and Network Security.