A NOVEL PROTOCOL FOR INDIRECT AUTHENTICATION IN MOBILE NETWORKS BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

[1]MS.P.G.RAJESWARI, [2]DR.K.THILAGAVATHI

[1]Assistant Professor, Department of Mathematics, V.L.B.Janakjammal College of Engineering and Technology, Coimbatore 42, Tamilnadu, India

[2]Reader, Department of Mathematics, Kongunadu Arts and Science College, Coimbatore 29, Tamilnadu, India

E-mail: drpgrajeswari@gmail.com , rajeswariphd@gmail.com

ABSTRACT

Unlimited mobility free of any fundamental communications is presented by Mobile Networks. In such networks, the information access between unacquainted nodes and server is a usual thing that happens frequently. This creates more chance to take the advantage of accessing information illegally by any invalid user node. The threat of apprehensive surroundings, information mishandling, etc is the eventual outcome. The fortification of classified and susceptible data in mobile networks can be done by the vital system, cryptosystem that spots the legitimacy. In such circumstances, the fundamental pre-requisite for better authentication is the performance of authentication by a middle agent, say Authentication server. Hereby, we are proposing a protocol that provides a secure transfer of information between the both unaccustomed parties. The most common public-key cryptographic scheme, elliptic curve cryptography is exploited to devise the protocol. Subsequently, the mobile networks employ the protocol for the authentication of user node. As the protocol utilizes the elliptic curve cryptography, it offers security more than enough with a reasonable key length. Hence the protocol develops an environment in which the user node which is unfamiliar to the Main server can transfer information without any eavesdropping of un-authenticated nodes.

Keywords: *Mobile Networks, Authentication, Indirect Authentication, Protocol, Elliptic curve cryptography (ECC), Elliptic curve*

1. INTRODUCTION

The fundamentals of data networking and telecommunication are being changed and integrated networks are becoming a reality owing to the wireless communication revolution. Personal communications networks, wireless LAN's, mobile radio networks and cellular systems, harbor the promise of fully distributed mobile computing and communications, any time, anywhere by freeing the user from the cord [1].

The mobile networking technology uses a radio transmission solution to support voice and/or data network connectivity. Mobile phone is a vital and the most commonly used application of mobile networking. Basically, the mobile networks, their wireless links and conventional stationary, wired computer networks are different. The communication is freed from the location constraints of the stationary wire line infrastructure due to the mobile connectivity, by which the user will be permitted to access the information anytime, anywhere [2].

A mobile network can be defined as an autonomous collection of mobile nodes which communicates over a wireless link. In other words it can be said as a radio network which is made up of a number of radio cells and each of the cells were served by a fixed transmitter. The transmitter is nothing but a cell site or base station. A mobile network has several advantages which include: increased capacity, reduced power usage and better coverage. These advantages make mobile networking pertinent to various real time applications. An important application of mobile networking is the mobile phone. A mobile phone is a portable telephone which uses a cell site (base station), or transmitting tower to receive or make

Vol6. No1. (pp 056 - 066)

calls. The signals are transferred to and from the cell phone using the radio waves [3].

In mobile networking, we have several security issues. The communication channel employed in mobile networks is air which provides plenty of possibilities for information snoop from nodes by un-authorized base stations that are pretending as the valid one, thus being the reason for the several security issues. Hence, to have reliable proper security over the mobile networks it is necessary to provide certain security measures, e.g., confidentiality, authenticity, and no traceability [4].

There are five main security services need to be considered in mobile networking namely: authentication, confidentiality, integrity, non-repudiation, availability. Authentication means that communicating partner knows the correct identity. Confidentiality means that unauthorized party is prevented from accessing certain message information. Integrity means that during communication, the message is unaltered. Non-repudiation means that the origin of a message having sent the message cannot deny it; Availability means that in all kinds of attacks, the normal service provision is in face [5]. Among the five security services, authentication is somewhat complex as well as the important one in mobile networking.

The act of authentication establishes or confirms something (or someone) as authentic, that is it verifies whether the claims made by or about the thing are true.

Protection against replay attacks; confidentiality, resistance against man-in-the-middle attacks etc are some of the several requirements for authentication. The security services to be provided in the authentication protocols specify such protection. The networking environment can be made more secure for information transfer by a better performing authentication protocol.

In addition to this, the node that wants access the server is new to the server. The Main server, a general service provider in networking area, doesn't have any information about the node. So, the involvement of intermediate is mandatory for authentication. This kind of authentication is so called indirect authentication. So to deal with our problem, the protocol we have developed is based on indirect authentication and so the Main server can authenticate the user node effectively with the help of a midway-agent called Authentication server.

The protocol derived from the cryptographic schemes, particularly public-key systems has a superior performance. The class of public-key cryptography contains the authentication protocol using RSA algorithm. It has a very good performance as it depends on the formation of mathematical puzzles that are complicated to unravel lacking definite information regarding how they were formed. Nevertheless, the RSA keys must be as a minimum 1024 bits long in order to offer ample protection. Recently, ECC's enhanced security with lesser key size feature has increased its popularity in cryptosystems. Elliptic curve cryptographic schemes belonging to public-key mechanisms and the RSA schemes are functionally identical. In comparison to the RSA schemes, Elliptic curve systems assist in achieving the desired security level with considerably smaller keys. For instance, in comparison to a 1024-bit RSA key, ECC presents identical level of security with a 164-bit elliptic curve key. Some of the momentous advantages of utilizing smaller keys are speed and efficient use of power, bandwidth, and storage. In our paper, we propose an efficient authentication protocol derived from ECC, a public key system that in comparison to the RSA algorithms, offers a reasonable security with lesser key length [6].

Eventually, our protocol follows indirect authentication and utilizes ECC for keys pair generation and hence it will authenticate a user node whether it is a valid or not. The remaining part of the paper is organized as follows. In section 2, the focus is on the works that were carried out in the past and section 3 deals with the concepts of authentication, its factors and indirect authentication. Some fundamental details of ECC and mathematical concepts of elliptic curves occupy Section 4 and the proposed protocol with an illustrative flow, generation procedure of key pairs, procedural steps and determination of certification code constitute Section 5. Section 6 details the implementation and results and Section 6 concludes the paper with the features of our protocol.

2. RELATED WORKS

Armando Fox and Steven Gribble, have described an implemented indirect protocol called Charon, which provides authentication and secure communication to clients by leveraging the strong protocol and deployed infrastructure of Kerberos IV. Charon consists of a portable proxy module that runs as untrusted, unprivileged code, and an extremely lightweight client module that runs quite efficiently even on their Sony MagicLink PDA.

Vol6. No1. (pp. 056 - 066)

Charon's security is at least as strong as that of Kerberos--the user's password never leaves the mobile device, and Charon cannot obtain Kerberos services for the user without the user's explicit cooperation on each request. Charon allows the mobile device to function as a smart card. They described their implementation of the protocol and a sample secure rlogin application, and also described how Charon can be used to implement cross-roaming agreements between mobile computing domains [12].

Eyk Hildebrandt and Gunter Saake, have shown that user authentication in MDBS is more complex than in traditional systems. Nevertheless, they have presented several approaches to resolve the problems with respect to different architectures and requirements. As a foundation they have introduced a user concept for MDBS as well as a policy for the granting and withdrawal of identities in such systems [23].

Michele Bugliesi, et. al., have studied the roles of message components in authentication protocols. In particular, they have investigated how a certain component contributes to the task of achieving entity authentication. To this aim, they have isolated a minimal set of roles that enables them to extract general principles that should be followed to avoid attacks. Then they have formalized certain principles in terms of rules for protocol parties and proved that any protocol following these rules will achieve entity authentication [24].

Jabeom Gu, et. al., have proposed an authentication framework, which uses PKI-based mutual authentication to establish trust relations between the communication entities and to guarantee minimized handover delay by extending the trust relations [25].

Vipul Gupta et al. [26] have studied the performance impact of using ECC 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.

Dawit Getachew et al. [27] 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. PSO shares many similarities with evolutionary computation techniques such as Genetic Algorithms (GA). The system is initialized with a population of random solutions and searches for optima by updating generations. However, unlike GA, PSO has no evolution operators such as crossover and mutation. In PSO, the potential solutions, called particles, fly through the problem space by following the current optimum particles.

Aytunc Durlanik et al. [28] have proposed an approach for secure SIP (Session Initiation Protocol) authentication by using a public key exchange mechanism using ECC. 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.

Tsuyoshi Abe, et. al., have implemented an identity provider (IdP), which was defined by the Liberty Alliance on a mobile phone. They have proposed an authentication method, which uses the personal IdP as a security token to prevent password leakage. In their method, the personal IdP on a mobile phone issues a security assertion signed by a private key on a Universal Subscriber Identifier Module (USIM). The method proposed by the authors has a unique feature that the initial authentication was performed on a user's mobile phone with the key pad as an input device and LCD as an output device [13].

V. Vijayalakshmi et al. [29] have proposed an authentication technique which makes use of 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

Vol6. No1. (pp 056 - 066)

minimum bandwidth, power, energy and computational speed.

3. AUTHENTICATION

The wired and the wireless network community are affected by one of the major security issues, Authentication [7]. Therefore, it is necessary to attain authenticity which is an essential prerequisite achieved by employing cryptographic systems in most applications where security matters. The integrated cryptographic systems satisfy all the above-mentioned requirements (authentication, confidentiality, integrity, non-repudiation, availability) [8]. Authentication is utilized as an initial process to authorize a mobile terminal for communication through secret credentials so as to provide security services in wireless networks [9].

Authentication can be defined as the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true [10].

A claimed identity is verified in this process i.e., someone (user, machine, etc.) is verified whether they are really the one who he/she/it claims to be.

3.1. Authentication factors

Strong user authentication is the term used occasionally to describe any authentication process that increases the probability of the correct verification of the identity of base station. Long complicated passwords or combination of two or more authentication factors are used to accomplish it.

In general, three authentication factors [11] are distinguished as:

- Knowledge factor – the user has to present the information known by him/her, i.e., some secret information such as, a password, PIN.
- Possession factor –the user has to present something possessed by him/her, i.e., some physical object for instance- tokens or keys.
- Being factor – In contrast to the former two factors, the user has to present something that is a part of him/her, for example- physical parameters. i.e., some biometric data e.g., fingerprint, iris pattern.

The most common case is the use of a password which is not really a good choice because passwords are typically short and easy to break. Challenge-response schemes, symmetric encryption, etc are some other more secure methods which use the public key cryptography.

The classification of the numerous authentication mechanisms and protocols that exist into two large groups, or patterns: Direct Authentication and Indirect Authentication is useful.

In direct authentication, pre-shared symmetric or asymmetric keys are utilized by the two parties for verifying each other and the flow of data between them. Whereas, a trusted third party, i.e. a Certification Authority, is made responsible for certifying one party to another party in the indirect authentication [7]. As the node and the Main server, both are not familiar to each other, we are proposing Indirect Authentication in our protocol. Succinctly, indirect authentication is suitable for this kind of situation.

3.2. Indirect Authentication

In both wired and wireless network, indirect authentication is the most widely used protocols. Indirect authentication means that entities use intermediary entities to authenticate each other [12]. A trust third party is involved in the indirect authentication protocol. Certification of the two communication parties is the responsibility of this third party such as certification Authority [13]. In indirect authentication, authentication server is commonly used to perform the authentication [14].

There are two authentication procedures in indirect authentication. When the user logs into his wireless device (such as mobile phones) it is the first phase. The authentication of the wireless device itself by the services is included in the second phase. As user interaction is not necessary, this method of authentication to the services is more flexible [14].

The authentication is efficient if and only the generated key pair shows utmost intricacy in hacking the generated key pairs by the adversaries. In our authentication protocol, we are using ECC for the generation of key pairs. The ECC is a suitable cryptographic scheme as it satisfies the necessary requirements for the authentication we are considered in our paper.

4. ECC

The emerging technology of ECC has replaced the traditional public key cryptosystems (RSA, DSA, and DH) [15]. The concern of instigating public key cryptography on mobile computing devices [16] has been addressed by the utilization

Vol6. No1. (pp 056 - 066)

of ECC. ECC (ECC) has two considerable merits: one is that it is well probed and so is extraordinarily safe and the other is that it requires a relatively shorter length than the other asymmetric systems [17]. Faster computations and lower power consumption in addition to memory and bandwidth savings result out of the advantageous characteristics of the ECC.

We start with the explanation of essentials of ECC and its mathematical formulations. The mathematical background of the ECC has been extensively discussed by the authors of [18] [19].

4.1. Fundamentals of ECC

A few basics of ECC that is necessary to comprehend the mathematical descriptions of elliptic curve utilized in the cryptographic scheme are discussed below:

Scalar: Any element is termed scalar if it is a constituent of either $GF(p)$ or $GF(2^k)$. The scalars are denoted using the lower case letter.

Scalar addition: Two or more scalars can be added to result in a new scalar. In case of $GF(p)$, the addition is performed using common integer addition modulo p which is comparable to polynomial addition modulo an irreducible polynomial of degree k, generating the field $GF(2^k)$. The scalar addition of two scalar r and s resulting in e is given by $e = r + s$.

Scalar Multiplication: two or more scalars can be multiplied to obtain a new scalar. In case of $GF(p)$, the multiplication is performed using common integer multiplication modulo p which is comparable to polynomial multiplication modulo an irreducible polynomial of degree k, generating the field $GF(2^k)$. The scalar e that denotes the scalar multiplication of two scalars r and s is given by $e = r \cdot s$.

Scalar Inversion: The denotation of multiplicative inverse of any constituent element of $GF(p)$ or $GF(2^k)$, a^{-1} has the property $a.a^{-1} = 1$. The computation of a^{-1} is done utilizing the Fermat's method or extended Euclidean algorithm.

Point: an ordered pair of scalars conforming to the elliptic curve equation is known as a point. Capital letter such as P_1, P_2, etc are used to denote the elements. Alternatively, a point P_1 is denoted as $P_1 = (x, y)$ where both x and y belong to the field. The coordinates x and y of point P_1 are denoted as $P_1 \cdot x$ or $P_1 \cdot y$, respectively for clarity.

Point Addition: Utilizing the elliptic curve 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. The symbol `+ ' in $P_3 = P_1 + P_2$ represents the elliptic curve addition. Point addition differs from usual scalar addition.

Point Multiplication: The multiplication of an elliptic curve point P by an integer e is denoted by $e \times P_1$. This is similar to the addition of P_1 to itself e number of times which results in another point on the curve.

Elliptic Curve Group: A special point called point-at-infinity is formed 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.

4.2. The mathematical theory behind elliptic curves

The theory presents a class of finite groups that have been established as quite appropriate for cryptographic use. In 1985, the utilization of elliptic curves in cryptography was independently recommended by Neal Koblitz [20] and Victor S. Miller [21].

The elliptic curves utilized in cryptography are defined on the basis of the 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}). The unimportant features are denoted as F_q, where $q = p$ or $q = 2^m$.

An elliptic curve is a locus of points in the elliptic curve whose coordinates conform to 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).

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

$$y^2 = x^3 + ax + b \quad (1)$$

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

$$y^2 + xy = x^3 + ax^2 + b \quad (2)$$

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

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

$$x_3 = \lambda^2 - x_1 - x_2 \quad (3)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (4)$$

where

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

Figure1 illustrates the addition of two EC points [22].

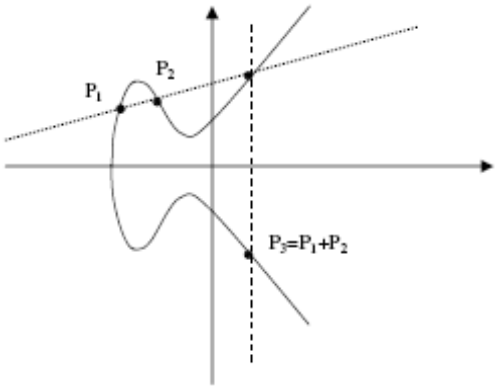

Figure 1: addition of two elliptic curve points

Assume two distinct points P_1 and P_2 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 is obtained as the reflection on the x axis of the third intersection, which is denoted as P_3. The set of points defined by the extended addition extended by the point ∞ forms an Abelian group [17].

Mathematical theory of elliptic curves provides a class of finite groups that have proven quite appropriate for utilization in cryptography. In addition, ECC is more suitable for authentication owing to some thriving features that are given below: [6]

- For a given key size, considerably greater security is provided by ECC.
- For a given level of security, the smaller key size also make much more compact implementations possible, i.e. faster cryptographic operations, running on smaller chips or more compact software is possible. In addition, less heat production and less power consumption is particularly advantageous in case of constrained devices, however, of some advantage anywhere.
- Extremely efficient, compact hardware implementations are available for ECC exponentiation operations which offer potential reductions in implementation footprint even beyond those due to only the smaller key length.

These features of ECC motivated us to provide a better authentication protocol between two unknown parties in the domain of networking. The protocol we have designed is discussed in the following section.

5. THE PROPOSED ECC BASED PROTOCOL FOR INDIRECT AUTHENTICATION

As stated earlier, in mobile networks the chance of accessing an unknown device is more. Before starting the transfer of information, authentication is very essential pre-requisite so that the information will reach a valid user node. As both the information requesting device (user node) and information provider (main server) are unfamiliar to each other, indirect authentication is more suitable option to provide authentication here. Based on the indirect authentication, an intermediate agent is used as a linking agent between both the user node and the main server in providing authentication. As by considering all the above concerns, we have developed the authentication protocol. The ECC shoulders well in the generation of keys pair for Authentication server as well as Main server. Using the generated key pairs, the authentication protocol will authenticate the user node. The subsequent sub-sections describe about the generation key pairs by ECC, flow of protocol, the authentication procedure and the determination of certification code.

5.1. Key pair generation

ECC is responsible for the Key pair generation which is the major area in our work where the elliptic curve participates. Key pair is only a combination of private key and a public key. Such a key pair is generated for Authentication server and for Main server. The generation of key pair can be mathematically derived utilizing the same as follows [6]:

In the rest of this paper, only the elliptic curves defined over F_p (where p is a "large" prime number) will be our focus. Integers in the range $0,1,\cdots,p-1,$ with the usual arithmetic modulo-p will naturally represent the field elements.

Let F_p be the prime finite field which is a set contributed by integers modulo p (where p is the random prime number). The following equation defines an elliptic curve E over F_p

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

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

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

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

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

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

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

As we know already, our protocol needs key pair for both the Authentication server and Main server. Hence, the private key chosen for Authentication server within the interval $[1, m-1]$ is $K_s(A.S.)$ and for Main server the private key is $K_s(M.S.)$ chosen from the same interval.

$$K_p(A.S.) = B * K_s(A.S.) \tag{9}$$

where $K_p(A.S.)$ is the public key of the Authentication server

$$K_p(M.S.) = B * K_s(M.S.) \tag{10}$$

where $K_s(M.S.)$ is the private key of the Main server

The properties of Elliptical curve aid in the eventual identification of the protocols parameters B, $K_s(A.S.)$, $K_s(M.S.)$, $K_p(A.S.)$, and $K_p(M.S.)$.

5.2. Flow of Protocol

A variety of signals have been transferred between the user node, Authentication Server and the Main Server. This procedural flow of signals will perform the checking of Authentication of the User node in the Main server. If the user is an authenticated one then the required information will be passed to the user from the Main server. Otherwise, a word of warning will be given to the respective user. The diagram that depicts the protocol flow is illustrated in the figure2.

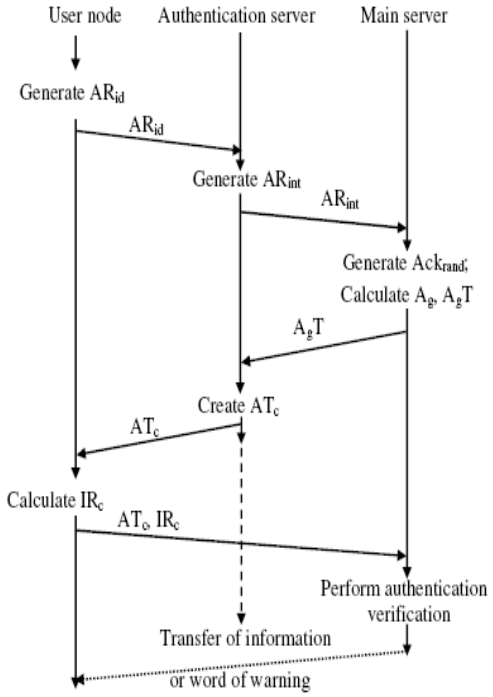

Figure 2: The Protocol designed for Indirect Authentication based on ECC

As per the protocol flow, the user will receive an Authentication Token after some interactions

between the user node-authentication server and Authentication server-Main server. After getting the Authentication Token from the Authentication server, the user node will generate an information request signal. The both will be sent to the Main server. The Main server will check whether the user node is an authenticated one or not. In response to this verification, either information or a word of warning will be passed to the user node.

5.3. Authentication procedure

The steps that are utilized in the authentication of a mobile user node can be categorized into three phases. The first phase consists of requesting for authentication, the second phase handles the authentication token calculation and its distribution and the final, third phase takes care of the authentication verification.

Phase I: - A mobile user node that wants to access information will request the Authentication server and hence the authentication procedure is initiated. This is done by generating AR_{id} , a random integer which is nothing but an identification number of the mobile user, which will be sent to the Authentication server. This request for information will be intimated to the Main server by the authentication server by sending an Authentication Request intimating signal AR_{int}, a random integer, to the Main server. When the Main server receives the intimating signal, it will immediately generate an acknowledging signal, Ack_{rand} , another arbitrary integer. Also, the Main server will generate Authentication go-ahead signal A_g as follows

$$A_g = B[AR_{\text{int}} * K_s(M.S.)] \quad (11)$$

where

$K_s(M.S.)$ is the secret key of the Main server

B is the Basic point

Along with this, the Main server calculates Authentication go-ahead token A_gT as follows

$$A_gT = [Ack_{rand} * K_p(A.S.) - AR_{\text{int}} * K_p(M.S.)] \quad (12)$$

where

$K_p(A.S.)$ is the public key of Authentication server

$K_p(M.S.)$ is the public key of service provider

This Authentication go-ahead Token will be utilized in future for authentication verification of the user node. Now, the Main server will keep the Authentication go-ahead Token A_gT itself and transmits the go-ahead signal A_g to the Authentication server and thus the first phase comes to an end.

Phase II:- In the second phase, the go-ahead signal is received by the authentication server from the Main server. Using that A_g the authentication server will calculate an Authentication Token for user AT_c and it is given by

$$AT_c = [AR_{id} + Ack_{rand} * K_s(A.S.)]B - A_g \quad (13)$$

This Authentication Token determined after the consultation of the Main server will be sent to the user which wants to access information. After the user node obtains the Token, Phase III of the authentication procedure will begin.

Phase III:- After obtaining the Token AT_c , the user will derive an information request signal IR_c as follows

$$IR_c = AR_{id} * B \quad (14)$$

Then the user node will send the Authentication Token along with the Information Request signal to the Main server. Now the Main server will perform the authentication verification using the certification code as follows

$$AT_c - A_gT = IR_c \quad (15)$$

When the equation (15) is balanced, the Main server will conclude that the node that tries to access is a valid one. If not, the user node is an adversary and so the Main server will respond to the node by any warning signal.

5.4. Determination of certification code

The certification code, the vital part of the authentication protocol is derived here in a step-by-step manner. The basic idea to be remembered is the signal which is transmitting from a source should remain same after it has been received by the destination. As this condition has been taken as an assumption, we are initiating the formulation by keeping the authentication request I.D. remains same at both the sending end, user node and the receiving end, Authentication server. This can be written as

$$AR_{id} = AR_{id} \quad (16)$$

Multiplying by the Basic point B on both sides,

$$AR_{id} * B = AR_{id} * B \quad (17)$$

Multiplying the same by $Ack_{rand} * K_p(A.S.)$ on either sides,

$$(AR_{id} * B) + [Ack_{rand} * K_p(A.S.)] = (AR_{id} * B) + [Ack_{rand} * K_p(A.S.)] \quad (18)$$

Equation (18) has been added by the $[AR_{\text{int}} * K_p(M.S.)]$ in both sides

$$(AR_{id} * B) + [Ack_{rand} * K_p(A.S.)] + [AR_{\text{int}} * K_p(M.S.)] = (AR_{id} * B) + [Ack_{rand} * K_p(A.S.)] + [AR_{\text{int}} * K_p(M.S.)] \quad (19)$$

This can be written as

$$(AR_{id} * B) + [Ack_{rand} * K_p(A.S.)] + [AR_{\text{int}} * K_p(M.S.)] - [AR_{\text{int}} * K_p(M.S.)] = (AR_{id} * B) + [Ack_{rand} * K_p(A.S.)] \quad (20)$$

From equation it can be written as

$$K_p(A.S.) = B * K_s(A.S.) \quad (21)$$

Substituting equation (21) in equation (20) will results in

$$\left((B * AR_{id}) + Ack_{rand} * B * K_s(A.S.)\right) - \left(AR_{\text{int}} * B * K_s(M.S.)\right) + [AR_{\text{int}} * K_p(M.S.)] = (AR_{id} * B) + [Ack_{rand} * K_p(A.S.)] \quad (22)$$

Equation (22) can be further modified as

$$\left(AR_{id} + Ack_{rand} K_s(A.S.)\right)B - \left(AR_{\text{int}} * K_s(M.S.)\right) * B + [AR_{\text{int}} * K_p(M.S.)] = (AR_{id} * B) + [Ack_{rand} * K_p(A.S.)] \quad (23)$$

Replacing $\left(AR_{\text{int}} * K_s(M.S.)\right) * B$ by A_g, equation (23) can be written as

$$\left(AR_{id} + Ack_{rand} K_s(A.S.)\right)B - A_g + [AR_{\text{int}} * K_p(M.S.)] = (AR_{id} * B) + [Ack_{rand} * K_p(A.S.)] \quad (24)$$

As it is noted in equation (13), equation (24) can be written as

$$AT_c + [AR_{\text{int}} * K_p(M.S.)] - [Ack_{rand} * K_p(A.S.)] = (AR_{id} * B) \quad (25)$$

This can be written as

$$AT_c - \begin{pmatrix} [Ack_{rand} * K_p(A.S.)] - \\ [AR_{\text{int}} * K_p(M.S.)] \end{pmatrix} = (AR_{id} * B) \quad (26)$$

Replacing the II term of L.H.S by $A_g T$ as already given in equation (12), equation (26) becomes

$$AT_c - A_g T = AR_{id} * B \quad (27)$$

By replacing the RH.S by IR_c, then the final equation will be

$$AT_c - A_g T = IR_c \quad (28)$$

This determination of certification code is construed as a proof and so it proves that the certification code is efficient in identifying the valid user node and it will neglect the information to any un-authorized node. Any imbalance in equation (28) intimates that any adversary user node is trying to access the Main server. Hence, here it is proved that no invalid user node will be allowed to access the Main server by using our Authentication protocol.

6. IMPLEMENTATION AND RESULTS

The protocol we have developed based on ECC for indirect authentication had been implemented in JAVA (Version 1.6). For the purpose of implementation, we have assumed some server systems for Main server and Authentication sever and client systems for Mobile user nodes. By using the key pair generation procedures we have generated public keys as well as private keys for both Main server and Authentication server. With the indirect knowledge of these keys only, the mobile user can access information; otherwise the Main server will not allow the user node to access information from itself.

As per the protocol flow, initially we made the user node to access the server by generating the identification number AR_{id} and sent it to Authentication server. Indirectly the main server sent its secret key $K_s(M.S.)$ to the Authentication server by the calculation of A_g. Then, the ATC is calculated by the authentication server, which is sent to the mobile user node so that the user node can contact the Main server for information. We have tested the protocol by this Authentication Token which was given by the Authentication server. It was clearly determined that the mobile user is the valid one by executing the certification code. The same kind of testing had been done for

different users who approached the Authentication server legally for access to the information. The Main server clearly authenticated their validation and allowed that users for information access if and only the certification code gets balanced. Along with this we have tested for invalid users also by randomly giving the Authentication token. As we have used ECC for generation of key pairs and the protocol we have designed was strong enough, the Main server easily determined its un-authentication and neglected information access and gave a word of warning signal to such kind of information snoopers. Thus we have implemented the protocol and we have observed its strict way of refusing information access to adversaries and allowing of information access to valid users.

7. CONCLUSION

The protocol we have developed offers reasonable security as it deploys ECC for key pair generation. Hence it is too difficult to break the key pair and so the protocol is hopeful in offering enough security. Also the designed protocol considers the strategies of indirect authentication leads to transfer of information between two unacquainted parties in a more secure environment. The performance of our protocol in some few steps adds additional advantage and hence the time consumption in execution of our protocol gets reduced. Thus it can be concluded that our protocol is a fortunate thing in avoiding the menacing effects of eavesdropping in mobile networks. Hence, the proposed protocol facilitates the achievement of a secure communication among two unknown parties in mobile networks with few simple steps and reduced computational complexity.

REFERENCES

[1] Xu Huang; Sharma, D., "Quantum Key Distribution for Wi-Fi Network Security", *In proceedings of 4th IEEE International Conference on Circuits and Systems for Communications*, pp: 85- 89, May 2008, Doi: 10.1109/ICCSC.2008.25.

[2] Hala Elaarag, "Improving TCP Performance over mobile Networks", *In proceedings of ACM Computing Surveys*, vol. 34, no. 3, pp: 357–374, September 2002.

[3] "Cellular Networks" from http://en.wikipedia.org/wiki/Cellular_network.

[4] V. K. Garg and J. E. Wilkis., "*Wireless and Personal communications Systems*", Upper Saddle River, NJ: Prentice-Hall, 1996.

[5] Shuyao Yu Youkun Zhang Chuck Song Kai Chen, "A security architecture for Mobile Ad Hoc Networks", *In proceedings of 2nd Computer Security Architecture Workhop*, October31, 2008.

[6] P.G.Rajeswari, K.Thilagavathi, "An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks", *In proceedings of International Journal on Computer Science and Network Security*, vol. 9, no. 2, pp:176- 185, Feb. 2009.

[7] Asad Amir Pirzada and Chris McDonald, "Kerberos Assisted Authentication in Mobile Ad-hoc Networks", *In proceedings of 27th Australasian computer Science Conference*, pp: 41-46, Dunedin, New Zealand, 2004.

[8] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh," Elliptic Curve Cryptography", *ACM Ubiquity*, vol. 9, no. 20, May 20 – 26, 2008.

[9] Ja'afer AL-Saraireh and Sufian Yousef, "Authentication Transmission Overhead Between Entities in Mobile Networks", *In Proceedings of International Journal of Computer Science and Network Security*, vol. 6, no. 3B, March 2006.

[10] Authentication from http://en.wikipedia.org/wiki/Authentication

[11] Boertien, N., Middelkoop, E.M., "Authentication in mobile applications", *Enschede: Telematica Institute*, 2001.

[12] Tsuyoshi Abe, Hiroki Itoh, and Kenji Takahashi, "Implementing Identity Provider on Mobile Phone", *In proceedings of ACM Workshop on Digital Identity Management*, pp: 46- 52, 2007.

[13] Fox, A. and Gribble, S.D., "Security on the move: Indirect Authentication using Kerberos", *In proceeding of the Second Annual International Conference on Mobile Computing and Networking*, pp: 155-164, 1996.

[14] Arto Hämäläinen, Pekka Jäppinen, Jari Porras, "Applying Wireless Technology to an Access control system", *White papers, Lappeenranta University of Technology*, September 2003.

[15] V. Gupta and D. Stebila and S. Fung, "Speeding Up Secure Web Transactions Using Elliptic Curve Cryptgraphy," *In proceedings of 11th Symposium on Network and Systems Security* , pp. 231-239, 2004.

[16] Manuel Barbosa, Andrew Moss, Dan Page, "Compiler Assisted Elliptic Curve Cryptography", *Lecture notes in Computer Science*, vol. 4804, pp: 1785-1802, November 21, 2007.

[17] 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.

[18] N. Koblitz. A Course in Number Theory and Cryptography. New York, NY: *Springer-Verlag*, Second edition, 1994.

[19] A. J. Menezes. Elliptic Curve Public Key Cryptosystems. Boston, MA: Kluwer *Academic Publishers*, 1993.

[20] N. Koblitz, Elliptic curve cryptosystems, in *Mathematics of Computation* 48, pp. 203-209, 1987.

[21] V. Miller, Use of elliptic curves in cryptography, *CRYPTO* 85, 1985.

[22] 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%20CR.pdf.

[23] Eyk Hildebrandt and Gunter Saake, "User Authentication in Multidatabase Systems", *In proceedings of 9th International Workshop on Database and Expert Systems Applications*, pp: 281- 286, 25- 28 August, Vienna, Austria, 1998, Doi: 10.1109/DEXA.1998.707414.

[24] Michele Bugliesi, Riccardo Focardi, Matteo Maffei, and Fabio Tudone, "Principles for Entity Authentication", *In proceedings of 5th International Conference on Perspectives of System Informatics*, vol. 2890, pp: 294- 306, Feb. 19 , 2003.

[25] Jabeom Gu , Sehyun Park, Ohyoung Song , Jaeil Lee , Jaehoon Nah and Sungwon Sohn, "Mobile PKI: A PKI-Based Authentication Framework for the Next Generation Mobile Communications", *In proceedings of Lecture Notes in Computer Science*, Springer- Verlag, vol. 2727, pp: 180- 191, 2003.

[26] Vipul Gupta, Douglas Stebila, and Sheueling Chang. "Integrating elliptic curve cryptography into the web's security infrastructure", *In proceedings of 13th International World Wide Web Conference on Alternate Track Papers and Posters*, ACM Press, pp: 402–403, 2004.

[27] Dawit Getachew, James H. Griner Jr., "An Elliptic Curve Based Authentication Protocol for Controller-Pilot Data Link Communications", *In proceedings of ICNS Conference & Workshop*, May 2- 5, Fairfax, VA, 2005.

[28] Aytunc Durlanik, and Ibrahim Sogukpinar, "SIP Authentication Scheme using ECDH", *In proceedings of World Academy of Science, Engineering and Technology*, vol. 8, October 2005, ISSN: 1307-6884.

[29] V. Vijayalakshmi and Dr. T.G. Palanivelu ,"Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks", *In proceedings of International Journal of Computer Science and Network Security*, vol.8, no.6, June 2008.