Incorporating Robust Authentication Scheme in P2P E-Commerce Applications

Chien-Hua Tsai,*, Pin-Chang Su

*a Department of Accounting Information, Chihlee Institute of Technology
b Department of Information Management, National Defense University

Abstract

Due to lack of effective trust management mechanism, heaps of deceptions exist in peer-to-peer (P2P) e-commerce (EC) environments, which seriously damage authenticity and availability of the systems. There are various challenges that are faced in the open autonomous environments. These existing challenges are mostly owing to the scarcity of correct authentication in P2P networks. Generally speaking, structured P2P networks are assumed to be accessible by allowing heterogeneous nodes or clients to interact and share one another. The identity (ID) authentication problem for this type of network has now become important. The paper presents a specific authentication key exchange scheme for P2P networks. Theoretic analysis shows that, a robust evaluation scheme based on elliptic curve cryptography (ECC) is proposed for P2P e-commerce networks with better secure identifying-and-authenticating features.

Key Words: Authentication, Peer-to-peer networks, Elliptic curve cryptography

Key Words: Authentication, Peer-to-peer networks, Elliptic curve cryptography

A 應用安全強固的驗證機制於對等互聯網路電子商務環境

蔡建華 * 蘇品長

*致理技術學院會計資訊系 b 國防大學資訊管理系

摘要

隨著點對點式（P2P）的技術崛起，使用者已運用這種互聯網的架構快速與便利的從事各種電子商務（EC）上的應用。雖然這種網路架構具有自我組織的能力和彈性，不過仍面臨來自開放通訊環境的威脅及挑戰，例如動態的拓撲結構、無線的連結、自主漫遊的環境，均暴露其危險與弱點。如何辨識身份及使用端互相確認，實為
1. Introduction

Peer-to-peer e-commerce networking has effectively become one of the most popular applications, and meantime the community itself is commonly perceived as an environment presenting both opportunities and threats. P2P networks typically exploit diverse connectivity between two or more participants over a network and the accumulated bandwidth of network participants rather than conventional centralized resources where a separate server computer provides service or applications (Friedman and Camp, 2005). A P2P network is the genus that does not have the notion of clients or servers but only equal peer nodes. In its plain form, networking is a fairly popular concept and seems benign enough in the past few years. Also, a P2P network can be an ad hoc connection, i.e., a couple of computers connected via wireless links to share files. Or, a P2P network can be a network on a much larger scale in which special protocols and applications set up direct relationships among users over the Internet (Stoica et al., 2001). Networks such as Napster, Gnutella, BitTorrent, eMule, Kazaa, and several other related systems make it easy for people to find what they want and share what they have. These systems provide a self-organizing platform for the construction of a variety of decentralized services, including network storage, content distribution, and application-level multicast (Dingledine et al., 2000; Ratnasamy et al., 2001; Rowstron and Pastry, 2001).

Although users benefit from an already existing file sharing network of computers using P2P technology, such networks disseminate huge security concerns. In a P2P environment, access rights are governed by setting sharing permissions on individual machines. When you download or transfer files from other peers, you don’t know for sure that the file is what it says it is. In effect, once you open the port you are no longer protected from malicious traffic coming through it. Such malicious behavior can take
various forms from storage flooding to denial-of-service (DoS) attacks, and users are especially vulnerable to become a victim of a security threat. Although numerous researches pay more attention to the security issues of the P2P networking communities, existing solutions have been subject to different secure settlements to different applications (Castro et al., 2002; Sit and Morris, 2002) and are still quite limited. Under the circumstances, making these P2P systems secure is a significant challenge, such as hassle-free participation of peers or sharing of sensitive data. In particular, when P2P systems are to be widely deployed on the transparent network substrate, they must be robust against malicious nodes that might try to provide anonymous communication. Many anonymous communication protocols were proposed for initiator and responder. Those protocols do not take trust into consideration. Therefore, the identities of peers have to be exposed over insecure channel and the privacy of peers is not protected.

Providing peer privacy in the P2P network has always been of vital importance, which poses even more challenges when facing a P2P system over the commercial Internet. As the network user base grew, less and less responsibility for administration was placed on the edges of the network, e.g., managing cryptographic keys. Recent works have shown that P2P systems are highly vulnerable to various security threats due to their inherent characteristics (Lee and Kim, 2003; Xiao et al., 2003; Takano et al., 2006; Lu et al., 2007; Chou et al., 2007). Of course, many other issues (Zhou and Haas, 1999; Weimerskirch and Westhoff, 2003; Milanovic et al., 2004; Gorantla et al., 2005; Li et al., 2006; Wong and Stajano, 2007; Bresson et al., 2007; MacQuire et al., 2008) exist that could be classified as security issues, such as routing, scalability, quality of service, and security framework, that will not be considered in this paper.

What we need is an authentication technology that conveniently allows both coarse and fine-grained control of who is authenticated to access a peer’s services while still being able to work without an institutional infrastructure. To provide strong authentication, called challenge-response authentication scheme is utilized into P2P system. The authentication of Groove (Groove Networks, 2002) has two different purposes. One is that their scheme binds users to their electronic identities, and the other is that link actions; such as modification to file, chat message and keystroke to electronic identities. In the meantime time, the authors of FL02 (Fahrenholtz and Lamersdorf, 2002) proposed a solution of strong authentication based on reputation management system with public key infrastructure (PKI).

Modern electronic commerce (EC) typically uses the Internet or other computer
networks in the transaction lifecycle, and involves the buying and selling goods or delivering services. There are a variety of different types of EC according to what their relationship is with the program such as B2B, B2C, C2C, G2B, G2C and P2P in particular. EC generally consists of the exchange of data to facilitate the business transactions between various parties. P2P is not only an EC type but also a technology that allows peers transact exchanges of information or computer resources without going through a central server. Since no intermediary is required, the type of EC is subject to ID-aware multiple threats in security. As mentioned under the unsecured issues, several P2P systems have been designed for the censorship-resistant form to block or accept requests from peer neighbors.

We explore a possibility of the identity of the peer node it is communicating with, thus designing an authenticated key exchange scheme that can be implemented in a pre-shared key model which forthright uses the stored knowledge in advance to accelerate the mutual authentication in the P2P networking structure. Our approach also provides end-to-end authentication with ID-based encryption and can simultaneously defend leakage of user’s identity against malicious attacks. Of course, we also attest that our scheme is efficient in pertaining to other measures, including both communication complexity and computational efficiency. This paper renders a P2P network security susceptible to link attacks. Therefore, it is desirable for the mechanism to adapt to other wired and wireless network frameworks with moderate modifications.

2. Background

In the section, we will first expound a little more issues regarding authentication service categories in P2P systems. Subsequently, we indicate that the existing nature of the P2P network is subject to security concerns involving identity management, malicious depredation, peer authentication, personal privacy and so forth. Particularly, identity management and peer authentication are flawed with unauthorized system access rights and disruption actions. In regard to this we use an identity of the peer nodes to act as certificate authorities in the communication facilitating fair authentication. These techniques and means of security thereof are the focus of this paper and are described in Sections 3 and Section 4.
2.1 P2P authentication requirements

Web services introduce new business opportunities and have influenced current computing models among applications and systems. This trend has reshaped the P2P various types of services to deal properly with interoperability requirements. Consequently, the P2P application environment needs an accommodative authentication scheme which can satisfy a great diversity of services so as to provide an effective, appropriate and secure platform such as strong authentications, robust accountability, mutual authenticity, authorization capability, adaptability and so on (Lua and Crowcroft, 2004). However, things in convenience have their pros and cons. On the one hand P2P networking employs a distributed application architecture that provides peculiar advantages of extensibility and flexibility, but on the other hand the architecture faces problems with security due to the autonomous nature in the system. For instance, attestation of identity authentication and digital message transmission are associated with high energy consumption costs, scalability problems and maintenance issues. Therefore, in order to enhance P2P application environment well, the elements of saving time-consuming tasks, accelerating attestation efforts and reducing certain dependency degrees from a certification authority need to be offered as the authentication requirements. To the best of our knowledge, there is barely relevant to the authentication measure which is able to fulfill the characteristic requirements including cost effectiveness, self-certified approach and pre-shared key (Su and Tsai, 2010). The requirements on the authentication functions for P2P systems are listed as follows.

(1) Strong authentication: Usually, strong authentication involves a multi-factor authentication approach to yield more protection for sensitive information, rather than by having simply used a username and password throughout. An effective strong authentication between individual peer must provide a related cryptographic process to facilitate e-commerce transactions. The authentication must establish a mutually protected tunnel to prevent possible attacks from successfully compromising the transaction between peers, such as man-in-the-middle (MITM), replay/preplay, and reflection attacks.

(2) Robust accountability: Accountability is a necessary requisition of information security and is being capable of tracking the source of each data occurrence. Existence of accountability mechanisms assures compliance especially for sensitive data access requiring prior authorization. Many different peers require the practicable cooperation of all involved parties. A robust accountability
mechanism must come up with the usage of trusted platforms to mitigate some of the possible risks existing in the confines of the P2P environment.

(3) Mutual authenticity: Peers or clients work together without hierarchy towards mutual authenticity and community in P2P systems. A mutual authenticity method authenticates the legitimacy of subscribers by transmitting authentication data between the entities. Every group member can verify the identity and authenticity of the peer each other by applying associated measures such as password, identifier and certification.

(4) Authorization capability: Authorization is the process by which a system allows the user access to various resources based on a particular authenticated user. Authorization capability depends on a secure authentication system to ensure that users are who he or she claims to be and accordingly prevent unauthorized users from gaining access to privileged resources. The design of the system is obliged to guarantee possible authorization capabilities according to certificates issuance or security clearances for online transactions among peers, as well as applying appropriate or legal policies to gain access.

(5) Adaptability: An adaptable scheme design can adapt to new changes incorporating any elements that would make it easy to implement new technologies in the future. For example, the selected wireless local area network (WLAN) technology must adapt to new users randomly joining the network to use applications that only require a slight adjustment. The scheme must be able to smoothly adapt to other P2P network systems without artificial modifications for a deployment environment as ad-hoc systems or other decentralized structures.

(6) Cost effectiveness: Mostly, security measures can sometimes affect system performance. The P2P system relies on resource contributions by the sharing peers. As the network increases the scalability, this potentially can lead to the problem of computing capacity, bandwidth consumption, and high-speed connectivity. Consequently, this design should be able to provide for suitably efficient and practical performance with strong reliability in the underlying business model for e-commerce.

(7) Self-certified approach: In the self-certified approach, communicating peers only use secret parameters while running their identity checks to ensure their compliance is as robust as possible, no more other trusted servers are required during the key agreement phase. To meet requirements of some e-commerce
transactions that do not submit an explicit certificate, a self-certified verification application which attests to the authenticity of the peer is supposed to be provided for reducing the risk of dependency degree on certification authority and possessing the high reliability with computational secrecy.

(8) Pre-shared model: Pre-shared model is a way both peers in negotiation use to identify themselves to each other with security and speediness, and it is typically easier to be configured at the peer end. As is well known, the purpose of authentication is that a peer can verify that someone is who they claim they are. In P2P systems, the process of authentication is typically based on either an encrypted time-stamp measure or a challenge-response method, called memorized password authentications, to speed up identifying peers across the Internet. Therefore, the authentication for P2P transactions must provide relatively quick proof of identity to decrease computation efforts and become a security liability under the negotiation.

2.2 P2P system and security

P2P networking technologies have gained popularity over recent years as a mechanism for users to share files without the need for centralized servers. As stated previously, the category of network uses various connectivity between participating nodes in a network and the cumulative bandwidth of network peers rather than customary centralized resources where a relatively low number of servers provide the core value to a service or application. Because of the characteristics of the P2P network itself, the security issues of the P2P network are of particularity and complexity such as routing security, encryption and decryption, identity management, malicious depredation, peer authentication, personal privacy and access control. The major security problem of the P2P network is peer authentication while nodes participate in the network.

Public key infrastructure provides an elegant way for addressing distributed authentication issues with P2P systems without an institutional authentication authority. In a PKI system with the use of X.509 certificates issued by peers optionally, users can gracefully handle the wide variety of certificate authorities to authenticate peer nodes. Usually, P2P users resort to a certificate authority to authenticate legal peers as the role of smart ‘servers’. However, authentication between two peers with no institutional infrastructure presents some concerned challenges based on such an authentication scheme as the number of nodes interacting with each other on a large scale. That is to say, no
node provides everlasting services in P2P networks since P2P networks are networks in which all nodes get in and out alternately. Because there is no central authority to manage consistent communal trusts, each peer in server mode needs to manage a database of certificate authorities for peers it is willing to allow to access its protected services. Therefore, the application of PKI to a P2P network is difficult such as identity management and trust authentication.

3. Our proposed scheme

Due to the lack of a centralized management, the P2P networks need more safety approaches to ensure peers and the architecture thereof to run smoothly. This work focuses on the mechanism for peer authentication. In this paper, we employ elliptic curve cryptography (ECC) schemes to design an efficient ID-based self-certified key exchange system in accordance with Miller (1986) and Koblitz (1987) studies, and present a solid authentication system on P2P networks. The proposed scheme is organized as follows: system setup, wrapper key computation, authentication, and session key generation, respectively.

During the initial stage, i.e., system setup phase, key generation center (KGC) defines system parameters and generates a secret/public key-pair that will be used to create self-certified public keys for the registering users. Please note that, it does not matter whether a fixed infrastructure (base station or central entity) or a mobile host (node or hub) is a prior knowledge in performing the peer challenge authentication from which the registration message has been received. With the usage of an origination by the registering user, KGC does not know the user’s master key during user registration and hence has no opportunity to masquerade as that user at a later time. According to the submitted identity information and the protected master key, KGC will return a self-certified public key and a witness for the public key to the registering user. Thereafter, the registering user can use his or her master key to derive a secret key from the witness issued by KGC. The remainder phases of the proposed scheme are described in detail as followings.

3.1 Setup phase

The KGC selects the parameters of elliptic curve domains and these specific items are defined geometrically with the underlying fields (Mitchell, 2003).
The field order $q$ which is used for the elements of $F_q$.

Two coefficients $a, b \in F_q$ that define the equation of the elliptic curve $E$ over $F_q$ (i.e., $y^2 = x^3 + ax + b$ in the case of a prime field).

The order $n$ of $P$, where $n = 4p_1 \times p_2 + 1$, $p_1 = 2p_3 + 1$, $p_2 = 2p_4 + 1$, and $p_1, p_2, p_3, p_4$ are all large primes.

When the system parameter $n$ is made in public, the prime numbers, $p_1, p_2, p_3, p_4$, can be discarded plainly. In the meantime, the KGC also chooses one-way hash function $H()$ and $h()$ both, and computes public key $Q_{KGC}$, such that
\[ Q_{KGC} = d_{KGC}P \]
where $d_{KGC}$ is the KGC’s secret key.

Suppose that a user $U_i$ wants to register with KGC. The procedure for user registration is stated as follows.

Step 1. $U_i$ takes the identification number $id_i$ and randomly choose a master key $d_i \in [2, n - 2]$ in order to obtain the signature $V_i$ of $id_i$. Compute
\[ V_i = h(d_i \mid\mid id_i)P, \]
then submit $(d_i, V_i)$ to KGC.

Step 2. KGC selects a random number $k \in [2, n - 2]$ and calculates a public key $Q_i$ and its witness $w_i$ for $U_i$ through the following equations
\[ Q_i = V_i + (k_i - h(id_i))P = (qixqiy) \]
\[ w_i = k_i + d_{KGC}(qix + h(id_i)). \]

Step 3. $U_i$ then derives a secret key $s_i$ as
\[ s_i = w_i + h(d_i \mid\mid id_i). \]
also verifies the authenticity of $Q_i$ by testing if
\[ S_i = s_iP = Q_i + h(id_i)P + (qix + h(id_i))Q_{KGC}. \]

Registration procedure must be in person or using the way to authenticate communication in some secure form. Moreover, each participant reliably knows a public key of KGC. Once all the users have registered and got his $(w_i, Q_i)$, the KGC does have no need to exist in the network. In the following, we show that the secret key $s_i$ and the public key $Q_i$ satisfy Eq. (6).
Proof. Eq. (4) is substituted for Eq. (5), then we obtain
\[ s_i = k_i + d_{KGC}(q_i + h(id_i) + h(d_i || id_i)). \]  
(7)

Both sides of Eq. (7) multiplied by \( P \) yield that
\[
\begin{align*}
    s_i P &= [(k_i + d_{KGC}(q_i + h(id_i)))P + h(d_i || id_i)P] \\
    &= [k_i + h(d_i || id_i)P] + (q_i + h(id_i))Q_{KGC} \\
    &= k_i P + V_i + (q_i + h(id_i))Q_{KGC} \\
    &= Q_i + h(id_i)P + (q_i + h(id_i))Q_{KGC}
\end{align*}
\]

This implies Eq. (6).

Although the information associated with participant users is stored in the KGC during the registration process, the KGC has to use both identities and the signatures, \((id_i, V_i)\), coming from communication peers to obtain the public key, \(Q_i\), which is derived from Eq. (3) and Eq. (4) as well as the secret key, \(s_i\), is produced in accordance with the KGC’s returned signature from Eq. (5) for our case. By such scheme, the KGC can not forge the public key itself without combined identity messages since any transmission relies on mutually checking computations, and these verification steps can prevent collusion in group members or between the KGC and peers. In the face of this collusion problem, the inspired rules continue to verify illegal keys that can be used to provoke a valid counterpart, and to avoid the conspiracy.

3.2 Wrapper key computation phase

In the second phase of the proposed work, we adopt an authentication mechanism (Su and Tsai, 2010) which is achieved in a single round trip to ensure trustworthy peers in P2P networks, and make it easily fit an off-line environment for fast identity checking and verification by reducing the number of key exchanges.

To do the single round-trip authentication, we assume that \(U_i\) and \(U_j\) are two users, and both of them would like to communicate with each other privately on public telecommunications systems. \(U_i\) sends \((id_i, S_i, Q_i)\) to \(U_j\) as well as \(U_j\) sends \((id_j, S_j, Q_j)\) to \(U_i\). Before generating the wrapper key, \(U_i\) and \(U_j\) require certifying that \((id_i, S_i, Q_i)\) and \((id_j, S_j, Q_j)\) are not comprised, and the messages also need to be sent right from their own entities, who represent legitimate individuals by checking Eq. (8) and Eq. (9) as below.
\[
\hat{S}_j = Q_j + h(id_j)P + (q_j + h(id_j))Q_{KGC}
\]  
(8)
Accordingly, \( U_i \) and \( U_j \) compute the wrapper key \( K_{ij} \) respectively, as the following equation:

\[
K_{ij} = d_i Q_j = d_j Q_i.
\]  

(10)

By using the wrapper-based ingredients, the architecture can provide great functionality in a secure manner.

### 3.3 Authentication phase

To be properly authenticated, the subject is usually required to provide another piece to the credential set. These credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. \( U_i \) and \( U_j \) therefore share a previously known wrapper key \( K_{ij} \) from the preceding phase. At the stage, the underlying design of ours is to use a challenge-response-type protocol as the method of compare and match. The procedure is separated into three distinct measure steps for credentials matching.

**Step 1:** \( U_i \) randomly picks up a \( t_i \in Z_q \), and calculates

\[
T_i = t_i P, \\
V_i = K_{ij} + T_i
\]

(12)

then sends \((id_i, V_i)\) to \( U_j \).

**Step 2:** Upon receiving the request, \( U_j \) haphazardly chooses a gained \( t_j \in Z_q \), and computes likewise

\[
T_i = t_j P, \\
V_i = K_{ij} + T_i
\]

(14)

Meanwhile, \( U_j \) decrypts \( T_i \) with the wrapper key as \( \hat{T}_i = V_i - K_{ij} \). In case an adversary might compromise \( T_i \), we mark the decrypted \( \hat{T}_i \) as \( \hat{T}_i \). With \( \hat{T}_i \) obtained, \( U_j \) is able to get the Diffie-Hellman key as \( W_j = t_j \hat{T}_i \). Besides obtaining the session key, \( U_j \) also needs to get \( Auth(B) \) and \( Auth(A)^* \) for authentication purpose, where

\[
Auth(B) = H(id_i, id_j, W_j),
\]

(15)

\[
Auth(A)^* = H(id_i, id_j, Z_j),
\]

(16)
Incorporating Robust Authentication Scheme in P2P E-Commerce Applications

where \( Z_j = W_j + K_{ij} \).  

Afterwards, \( U_j \) sends \((id_j, V_j, Auth(B))\) to \( U_i \).

Step 3: After getting the request, \( U_i \) has virtually collected all in need of generating the session key. First, \( U_i \) checks if \( Auth(B) \) from \( U_j \) matches \( Auth(B)^* \) by reckoning

\[
\hat{T}_i = V_i - K_{ij}
\]

where \( \hat{T}_j = W_j - T_{\hat{T}_j} \).  

\[
Auth(B)^* = H(id_i, id_j, \hat{W}_j)
\]

If so, \( U_i \) then continues calculating the session key and \( Auth(A) \) as the following formulas:

\[
Z_i = \hat{W}_j + K_{ij}
\]

\[
Auth(A) = H(id_i, id_j, Z_i)
\]

Otherwise, \( U_j \) cannot be authenticated, and the service fails to respond to a handshaking. At last, \( U_i \) returns \( U_j \) to \( Auth(A) \) for authenticating himself or herself. If \( Auth(A) \) matches \( Auth(A)^* \), the whole authentication process is thereupon accomplished.

3.4 Session key generation phase

The authentication processes of Section 3.2 and 3.3 are for first-time communication users who are the unrecognized both sides. While the transmission channel is established via the wrapper key, the stealth message is exploited to authenticate the identity of two communicating parties in a secured manner. The purpose of this stage is to prevent from the replay or forgery attack by mutual authentication. In order to withstand the attacks, the timestamp is added to the message as a nonce code for generating the current session key to enable the users to have secure communications with each other.

For a safe communication channel to be in place, session keys need to be generated in a security in their hashed version between two users. Throughout each session, the key is transmitted along with each message and is encrypted with the recipient’s public information.

In our case, session keys must be chosen randomly so that they are unpredictable by an attacker. Therefore, \( U_i \) and \( U_j \) generate their session keys \( SK_i \) and \( SK_j \) respectively by using the following expressions.
\[ SK_i = H(id_i, id_j, T_i, \hat{T}_j, \hat{W}_j) \]  
(23)

\[ SK_j = H(id_i, id_j, \hat{T}_i, T_j, \hat{W}_j). \]  
(24)

By enclosing substance encrypted with this sort of the hash value, the use of wrapped session keys keeps the private information even more secret, and these attacks are much more difficult over the network.

3.5 Membership update phase

With the lapse of time, some users will revoke their registrations, whereas others may have an issue with new member registrations. Registration for all new members and revocations for current members, there will be no additional operations to perform membership update each communication, only in a regular or casual way to fulfill the requirements. Under the circumstances, the wrapper keys stored in the system will be timely renovated to provide better efficiency and to facilitate the authentication process.

4. Security evaluation of our scheme

In this section, we first describe that the security of our proposed scheme is computationally related to ECC. We demonstrate that the proposed authentication scheme is correct and achieves the security requirements of authentication functions. Then we evaluate the performance of our scheme and compare it with some previous works.

4.1 Security under ECC

The elliptic curve analog as mentioned above is exposed to a similar attack, in particular, if any redundancy exists in the representation of the elliptic curve point, even ciphertext leaks some kind of information in a careless way. The inherent strength of the protocol follows from the difficulty of knowing which two points on a secure elliptic curve have been added to yield the resulting one. Therefore, the security of the elliptic curve cryptosystems depends on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP).

4.1.1 Strong authentication

X.509 describes two levels of authentication: one is a simple authentication, based on use of a password to verify user identity, and the other is a strong authentication, using
Incorporating Robust Authentication Scheme in P2P E-Commerce Applications

credentials created by cryptographic methods. The standard certificate format recommends that only strong authentication should be used as the basis of providing secure services. Our method adopts a strong authentication which is associated with additionally required factors to identity each entity.

In our method, if an attacker attempts an attack to disclose the information related to private key, \( d_i \) which is derived from the widely distributed (‘public’) key \((s_i, X_i, Q_i)\), then the attacker might potentially use the obtained \( d_i \) to play the role of \( U_i \), so as to forge a legitimate client. However, it is practically impossible to deduce the value of our private key from the value of the public key since the attacker must has the ability to solve the ECDLP which computes \( Q = dP \) for a given point \( P \).

4.1.2 Robust accountability

As services and computer resources of P2P services become increasingly non-local, accountability to users for the results and implementation status of the service have emerged as important issues. Our scheme presents a robust accountability method and discusses how authentication could be applied to data accountability.

When \( U_j \) sends \((id_j, V_j, Auth(B))\) to \( U_i \), an adversary can intercept the datum from the public channel and then plays the role of \( U_j \) to spoof \( U_i \) or other users to gain unauthorized access. The cheating behavior does not work and is unable to pass the verification of \( Auth(B) = H(id_i, id_j, \hat{W}_j) \) because the identification information \( \hat{w}_j \) is needed as an input parameter for the one-way function \( H() \), and it will be used in the operation \( Auth(B) = Auth(B)\) to verify the identification of every user.

4.1.3 Mutual authenticity

The mutual authentication is a security feature in which authenticity of a peer is verified after each fixed time interval by the peer station during conversation or progress of a service. In our case, when peers are attempting to establish a connection, their identities of the peers are authenticated each other suitably by applying public/private key-pairs, identifiers and certified credentials.

In addition, based on the Diffie-Hellman key agreement protocol, our method uses a wrapper key as authentication information, encryption seed, and a factor for derivation of the final session key. With the wrapper key protection, it prevents the key exchange process from the man-in-the-middle attack, to which the Diffie-Hellman protocol alone is vulnerable. Although an attacker might get the information of \((s_i, X_i, Q_i)\) and \((id_i, V_i\),
from the public channel, the attacker still cannot derive each peer’s secret key from the public key as mentioned in the preceding section. Accordingly, an adversary does not have any opportunity to obtain the common session key shared between any two of them.

4.1.4 Authorization capability

In some situations, the standard authorization rules, known as access control list (ACL) policies and protected object policies (POP), might not be able to express all the conditions required by a P2P’s security policy. This paper provides an optional external authorization capability by reliable peer-initiated connections to automatically approve or deny any additional authorization requirements.

In the proposed mechanism for authorization services, an initiator can confirm that the intended recipient of the shared key actually processes the shared key by verifying the second message, but the respondent cannot realize initiator’s key confirmation. Our countermeasure can effectively help prevent like denial of service attacks because of the corresponding property in the wrapper key. That is, an adversary cannot wildly guess the valid wrapper key within a probabilistic polynomial time since the authorization will need to initiate the key exchange for a security service between the initiator and the respondent.

4.1.5 Adaptability

P2P systems should offer more freedom of interaction structures in decentralized problem solving between peers. Due to lack of a mechanism to gather the exchange information in unstructured and structured topologies back and forth, existing P2P systems may not be well equipped so as to make them adapt worse to high flexibility. In the proposed paper, no matter what P2P paradigms are taken advantage of each, the authentication measure is fully adaptable to dissimilar environments without requiring human intervention.

When an adversary intercepts a stream of messages from \( U_i \) to \( U_j \) and plays back the stream to the two peers, our approach can identify this fraudulent signature and helps prevent this sort of attack throughout the duration of the connection in unstructured or structured P2P systems. Regardless of interaction circumstances, the replay attack is thwarted since the proposed scheme adds a signed message ID to request messages and expects a signed relates-to header on response messages. Consequently, the hash-lock (i.e., challenge-response) message cannot be replayed as a response.
4.1.6 Cost effectiveness

Although P2P systems provide a convenient platform for distributed applications, the problem of time-consuming computation and high-speed connectivity is hard to tackle good performance while the system’s participants are gradually increasing. Resource consumption has to maintain the minimal overhead requirements and achieve efficient fulfillment for the peers.

To deliver better performance with such an infrastructure in P2P systems, our approach proposes a specific authentication key exchange scheme that thoroughly employs the difficulty of the ECDLP. Due to the underlying of the ECC group structure, the computational complexity for breaking the elliptic curve cryptosystem with an elliptic curve key size of only 150 bits (Lenstra and Verheul, 2001), using the Pollard method, is $3.8 \times 10^{10}$ MIPS (Million Instructions Per Second years). In comparison, the fastest method to break RSA, using the General Number Field Sieve Method to factor the composite integer $n$ into the two primes $p$ and $q$, requires $2 \times 10^8$ MIPS-years for a 768-bit RSA key and $3 \times 10^{11}$ MIPS-years with a RSA key of length 1024. Therefore, it is clear that ECC-based way fairs better than RSA-like manner in terms of cost effectiveness in authentication.

4.1.7 Self-certified approach

On the one hand having a distributed application structure offers a portion of resource services between P2P participants, on the other hand increasing the possibility of illegal access from malicious intruders is raised to the networking community, such as password guessing, password-compromise impersonation (PCI) and unknown key-share (UKS) attacks. Moreover, an intruder might try to impersonate KGC by determining a relationship from the public message.

Our scheme introduces a self-certified approach, known as a public key authentication cryptosystem, and makes it resistant against the foregoing attacks. In this mechanism, each peer obtains a valid certificate along with corresponding identity information, and holds one session key of the participants. The session key ensures peers’ communication against any possible attacks, and even the KGC doesn’t collude. Messages sent between the communication peers are self-certified, and hence, the certificates can be used to verify the identities if applicable. Additionally, the proposed measure supports off-line identity assurance besides on-line identity verification. That is, each peer can rely on KGC’s public key to reliably verify the authenticity of each participant identity. It is effective to avoid
untrustworthy KGC misappropriating the user’s secret key.

We say that a self-certified scheme is presently counterfeited against adaptive chosen message attack if no polynomial bounded adversary A has a non-negligible advantage against the challenger in the following game: The challenger takes a security parameter $d'_i$ and runs the setup algorithm. It gives the adversary the resulting system parameters and a public key $Q_i$ of the certificate authority. If an attacker attempts to carry out an attack by revealing the private key $d_i$ from the public key of the $Q_i$, then he or she can play the role of $Q_i$ to forge. In case of that, the attacker must solve the ECDLP given by $Q_i$ to determine $d_i$.

4.1.8 Pre-shared model

The purpose of authentication is not only authentic to verify that peers are who they claim to be but also swift to confirm that the origin of a peer is a trusted one particularly in a P2P environment. In this paper, we propose the property for identity authentication, which is a pre-shared way and can accelerate the mutual authentication in the P2P networking structure.

When applying the scheme, the information of the reciprocal wrapper key $K_{ij}$ is stored in a specific space with necessary protection through the system access respectively. The mechanism forthright uses the stored knowledge in advance for session key generation process between two communicating peers that know each other. In this way, if a participating peer is aware of the improper message from another peer in the P2P network, the manual communication progress is then discontinued instantly and the authentication process is unsuccessful.

4.2 Comparison of methods for P2P authentication

In this section, we compare the authentication effectiveness of our method with other algorithms. The comparison is performed whether the scheme satisfies the requirements for P2P authentication or not. The result of comparison is summarized in Table 1. In the Table, symbols: $\bigcirc$, $\triangle$, and $\times$ that mean the degree of supporting the component of requirements by each corresponding scheme: support, partially support and no support, respectively. Compared to the existing schemes, our method presents more astonishing characters in the foregoing authentication functions. Besides, we have synthesized the main advantages of our approach, and the benefits of these distinguishing characteristics are displayed in Table 2.
Incorporating Robust Authentication Scheme in P2P E-Commerce Applications

Table 1 The comparison of methods for P2P authentication

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong authentication</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Robust accountability</td>
<td>×</td>
<td>△</td>
<td>×</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Mutual authenticity</td>
<td>×</td>
<td>△</td>
<td>△</td>
<td>×</td>
<td>△</td>
<td>○</td>
</tr>
<tr>
<td>Authorization capability</td>
<td>○</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Adaptability</td>
<td>×</td>
<td>○</td>
<td>○</td>
<td>×</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Cost effectiveness</td>
<td>×</td>
<td>○</td>
<td>○</td>
<td>×</td>
<td>△</td>
<td>○</td>
</tr>
<tr>
<td>Self-certified approach</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>○</td>
</tr>
<tr>
<td>Pre-shared model</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>○</td>
</tr>
</tbody>
</table>

Table 2 The main advantages of the proposed scheme

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single round-trip authentication</td>
<td>The authentication only requires a single round trip to verify knowledge of the existing keys between peers. Without additional roundtrips, the key exchange is relatively short period of time.</td>
</tr>
<tr>
<td>Off-line self-certified operation</td>
<td>If the identity verification succeeds after the initial registration, communication peers can employ an off-line self-certified procedure to achieve the authentication without knowledge of the KGC.</td>
</tr>
<tr>
<td>Security to prevent data tampering</td>
<td>The security of the proposed scheme which is based on the difficulty of solving ECDLP and one-way hash function can provide various security protections from malicious attacks such as identity exposure, man-in-the-middle and replay/reflection.</td>
</tr>
<tr>
<td>Reduction of transmission to enhance efficiency and safety</td>
<td>Because of a single round-trip mechanism, reduction in communication through P2P networks can be used to perform an efficient authentication. The scheme can also diminish the possibility of data interception from data revealing the content of communications.</td>
</tr>
</tbody>
</table>

5. Conclusions

In summary, based on the results of ECC algebraic structure for simplifying public key distribution and bearing a great ID-based self-certified cryptosystem, the proposed scheme can not only gain much efficiency in saving the communication cost but also establish more secure channel. We have also taken into consideration several potential security issues in structured P2P overlay networks by analyzing security evaluation. Our approach can endure per attack and carry out correct critical message delivery under
these attacks. At present, public key cryptosystems maintain high security for many communication mechanisms. However, prevalent P2P networks have a prior assumption that any node expects to be accessible correctly. It is such an imperative problem in P2P e-commerce environments that a lot of various parties reside in open systems without pre-trust relationships and wish to communicate friendly.

This paper describes a new scheme for identifying any user who wishes to join a P2P network based on elliptic curve cryptography, and for authenticating a person’s identity coupled with a conscientious and careful process. Also, our method aims at presenting a strong-and-robust defense against unfriendly compromising intentions. The proposed scheme gives several notable advantages over the existing authentication methods: (1) the scheme constructs a fast and extremely secure identification system; (2) the scheme provides a robust authentication mechanism that checks for both public and private information; (3) the scheme verifies participant identities in pre-shared key model and uses smaller certificate sizes; (4) the scheme possesses a self-certified property and supports off-line identity verification. From our inference and analysis, we believe that the proposed scheme offers significant ameliorations in security, and can help improve the authentication performance of current and future P2P systems where mobilized users, shared resources and decentralized collaborative work spaces are naturally clustered.

References


Anonymity and Unobservability, Berkeley, California, 67-95.


