A Secure and Efficient Dynamic Identity based Authentication Scheme for Multi-Server Environment using Smart Cards

Chengbo Xu[1,2,*], Zhongtian Jia[3], Fengtong Wen[2] and Yan Ma[1]

[1]Institute of Network Technology Research, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]School of Mathematical Sciences, University of Jinan, Jinan 250022, China
[3]Shandong Provincial Key Laboratory of Network Based Intelligent Computing, Jinan 250022, China

[*]Corresponding author, E-mail: cbqysy@gmail.com

Abstract

Recently, more and more researches have been focused on proposing dynamic identity based remote authentication scheme for multi-server environment. In 2011, Lee, Lin and Chang proposed an improved scheme to remedy the weaknesses of Hsiang-Shih's scheme. However, we observe that Lee-Lin-Chang's scheme is still vulnerable to stolen smart card attack and malicious server attack. Besides, the password change phase of Lee-Lin-Chang's scheme is neither efficient enough nor convenient to users. In this paper, we propose an improved scheme to remove the aforementioned weaknesses and simultaneously not to decrease other security features. In the proposed scheme, there is no useful information can be obtained from the values stored in smart cards. Thus the stolen smart card attack can be blocked. To avoid malicious server attack, we move the user authentication process from service providing servers to the registration center, which can ensure each server has a different secret key. Through comparing with several schemes proposed recently, we demonstrate our proposed scheme is more secure and efficient. Therefore, the proposed scheme is more practicable.

Keywords: *Authentication; Dynamic identity; Multi-server; Password; Smart card*

1. Introduction

Nowadays, the Internet has become an integral part of our everyday life. Online, we can easily access interesting services provided by remote service providing servers at any place or time. At the same time, network security becomes an important issue in the public communication environment. Remote user authentication is an important mechanism that provides the conformation of two communication parties' identity.

In 1981, Lamport [9] proposed the first well-known password based remote user authentication scheme. However, the server must store a password list and consequently cannot resist interpolation attacks. Since then, numerous smart card based remote authentication schemes [2, 6, 7, 8, 13, 17, 19, 20] have been proposed to improve security and efficiency features in the remote authentication process. However, all these schemes are designed for the single-server environment.

Due to rapid growth of computer network, many network environments have been becoming multi-server based. In multi-server environment, those conventional schemes aforementioned cannot be directly applied because each user not only needs to repetitively register at various remote servers but also needs to remember these numerous different identities and passwords. In order to resolve this problem, a serial schemes [1, 5, 12, 14, 18, 22] have been proposed for multi-server environment. In 2000, Lee and Chang [12] proposed a user identification and key distribution scheme based on the difficulty of factorization and hash function, which permits one-time registration at a registration center and many times access to services in all remote servers. One year later, Li *et al.*, [14] proposed a remote user authentication scheme by using neural networks. However, Li et al.'s scheme is impractical since too much time and cost are spent on training and maintaining the neural networks. To improve the efficiency, Lin *et al.*, [18] proposed a new remote user authentication based on discrete logarithm problem. Later, Juang [5] proposed an efficient multi-server user authentication and key agreement protocol based on hash function and symmetric key cryptosystem. However, Juang's scheme was still not efficient enough in password change phase, and could not against smart card stolen attack. Later, Chang and Lee [1] proposed a novel remote authentication scheme to remove the above defects in Juang's scheme. Actually, Chang and Lee's scheme is also not secure and was found vulnerable to insider attack, spoofing attack and registration center spoofing attack.

A common feature among all above mentioned schemes is that the user's identity is static in all the transaction sessions. In this case, an adversary can gather partial information about user's authentication message, and further use these information to trace and identify the different requests belonging to the same user. To overcome this risk, Liao and Wang [16] proposed a secure dynamic ID based remote user authentication scheme for multi-server environment. The security of this protocol is only based on a secure hash function. Moreover, it provides a secure method to update password without the help of any third trusted party. They claimed that their scheme can resist various attacks and can achieve mutual authentication and two-factor security. However, Hsiang and Shih [4] found that Liao-Wang's scheme is vulnerable to insider's attack, masquerade attack, server spoofing attack, registration center spoofing attack and is not reparable. Furthermore, Liao-Wang's scheme fails to provide mutual authentication. To remove these flaws, Hsiang and Shih [4] proposed an improved scheme. Unfortunately, Hsiang-Shish's scheme was pointed out still not secure and susceptible to replay attack, impersonation attack, stolen smart card attack, server spoofing attack and is not easily reparable. Besides, the password cannot update correctly according to Hsiang-Shih's scheme. To solve these problems, Lee, Lin and Chang [10] and Sood, Sarje and Singh [19] proposed their schemes respectively. In 2011, Li *et al.*, found that Sood-Sarje-Singh's scheme is vulnerable to leak of verifier attack and stolen smart card attack. To tackle these problems, they proposed their scheme, which has been pointed out still vulnerable to masquerade attack and replay attack by Han [3].

In this paper, we will point out Lee-Lin-Chang's scheme [10] is still not secure and vulnerable to stolen smart card attack and malicious server attack (A service providing server masquerades as other server to fool users, or masquerades as a user to fool other servers). In addition, the password change phase of their scheme is low efficient and inconvenient to users. To overcome these weaknesses, we propose a more secure and efficient authentication scheme based on dynamic identity for multi-server environment using smart card.

The rest of this paper is organized as follows: in Section 2, we provide a brief review of Lee-Lin-Chang's scheme [10]. Section 3 points out the security weaknesses of Lee-Lin-Chang's scheme. The proposed scheme and corresponding scheme analysis are presented in Sections 4 and 5 respectively. Finally, we conclude the paper in Section 6.

The notations used throughout this paper are summarized in Table 1.

Table 1. Notations

U_i	The i th user
S_j	The j th service providing server
RC	The registration center
ID_i	The identity of the user U_i
PW_i	The password of the user U_i
SID_j	The identity of the server S_j
x	The master secret key maintained by RC
y	A secret number known only to RC
b_i	A random number generated by RC for the user U_i
$CUID_i$	The dynamic identity generated by the user U_i for authentication
SK	A session key shared among the user, the server and the RC
N_{i1}	A nonce generated by the user U_i 's smart card
N_{i2}	A nonce generated by the server S_j for the user U_i
N_{i3}	A nonce generated by the RC for the user U_i
$h(\cdot)$	A secure one-way hash function
$\oplus$	Exclusive-OR operation
□	Message concatenation operation
$\Rightarrow$	A secure channel
$\rightarrow$	A common channel

2. Review of Lee-Lin-Chang's Scheme

In this section, we review the dynamic identity based remote user authentication scheme for multi-server environment proposed by Lee, Lin and Chang [10]. Their protocol includes four phases: registration, Login, verification and password change, and involves three entities: users, service providing servers and registration center. Registration center (RC) chooses the master key x and a secret number y which only RC knows, and then computes and shares $h(x \| y)$ and $h(y)$ with each server in a secure channel. The login and verification phases of this scheme are shown in Figure 1.

2.1. Registration Phase

When the user U_i wants to become a legal client to access the systems, he/she must register himself/herself with the registration center RC . The steps of the registration phase are as follows:

Step R1. $U_i \Rightarrow RC : ID_i, h(b \oplus PW_i)$. U_i freely selects his/her identity ID_i and PW_i , generates a random number b_i and computes $h(b \oplus PW_i)$. Then U_i submits ID_i and $h(b \oplus PW_i)$ to the registration center RC through a secure channel.

Step R2. RC computes $\mathrm{T}_i = h(ID_i \| x)$, $V_i = T_i \oplus h(ID_i \| h(b \oplus PW_i))$, $B_i = h(h(b \oplus PW_i) \| h(x \| y))$ and $H_i = h(T_i)$.

Step R3. $RC \Rightarrow U_i$: smart card. RC stores $\{V_i, B_i, H_i, h(\cdot), h(y)\}$ in a smart card and issues the card to U_i through a secure channel.

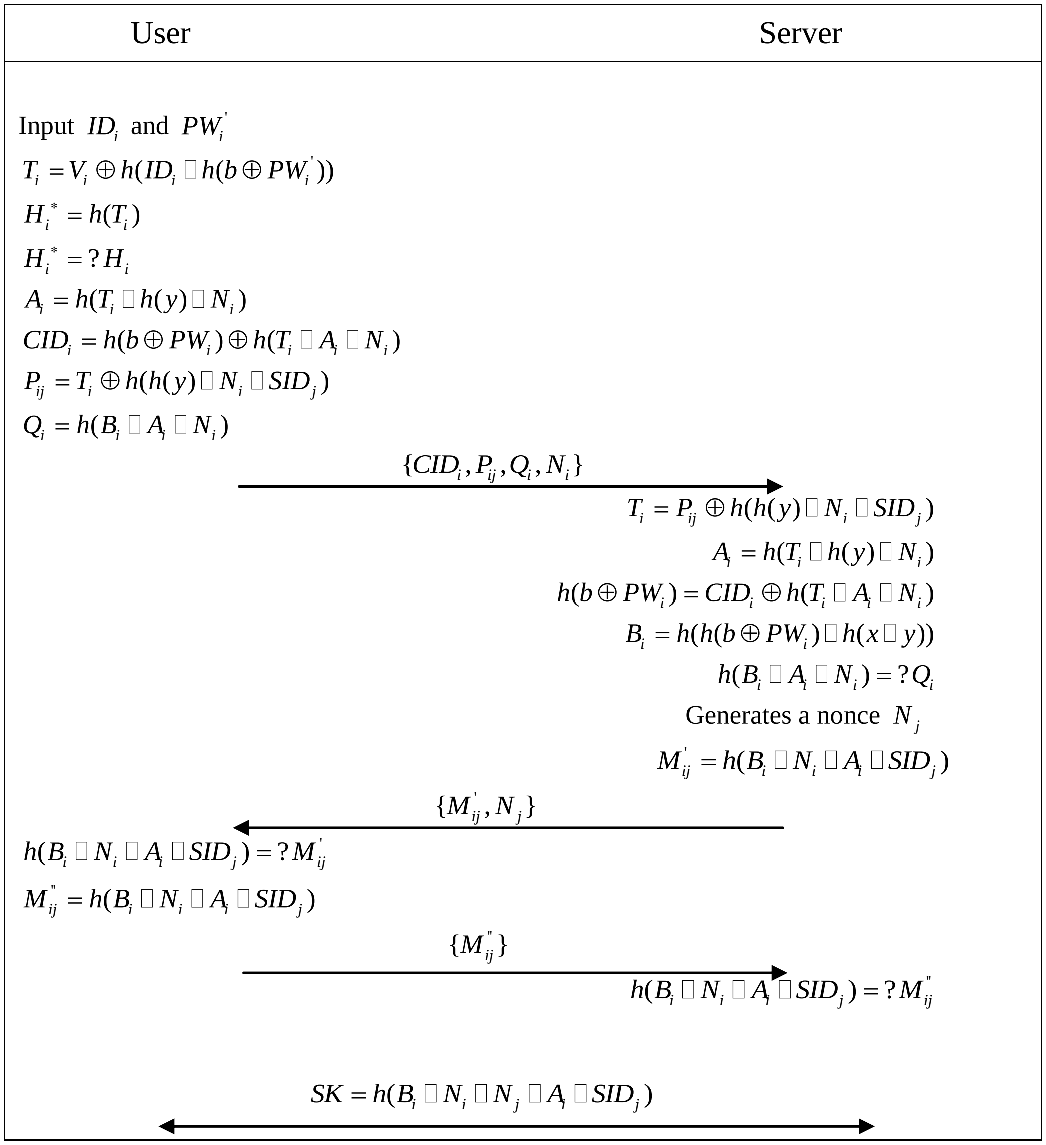

User
Server
Input ID_i and $PW_i^{'}$
$T_i = V_i \oplus h(ID_i \parallel h(b \oplus PW_i^{'}))$
$H_i^* = h(T_i)$
$H_i^* = ?H_i$
$A_i = h(T_i \parallel h(y) \parallel N_i)$
$CID_i = h(b \oplus PW_i) \oplus h(T_i \parallel A_i \parallel N_i)$
$P_{ij} = T_i \oplus h(h(y) \parallel N_i \parallel SID_j)$
$Q_i = h(B_i \parallel A_i \parallel N_i)$
$\{CID_i, P_{ij}, Q_i, N_i\}$
$T_i = P_{ij} \oplus h(h(y) \parallel N_i \parallel SID_j)$
$A_i = h(T_i \parallel h(y) \parallel N_i)$
$h(b \oplus PW_i) = CID_i \oplus h(T_i \parallel A_i \parallel N_i)$
$B_i = h(h(b \oplus PW_i) \parallel h(x \parallel y))$
$h(B_i \parallel A_i \parallel N_i) = ?Q_i$
Generates a nonce N_j
$M_{ij}^{'} = h(B_i \parallel N_i \parallel A_i \parallel SID_j)$
$\{M_{ij}^{'}, N_j\}$
$h(B_i \parallel N_i \parallel A_i \parallel SID_j) = ?M_{ij}^{'}$
$M_{ij}^{"} = h(B_i \parallel N_i \parallel A_i \parallel SID_j)$
$\{M_{ij}^{"}\}$
$h(B_i \parallel N_i \parallel A_i \parallel SID_j) = ?M_{ij}^{"}$
$SK = h(B_i \parallel N_i \parallel N_j \parallel A_i \parallel SID_j)$

Figure 1. Lee-Lin-Chang's Scheme

Step R4. U_i keys b into the smart card. Eventually, the smart card contains $\{V_i, B_i, H_i, b, h(\cdot), h(y)\}$.

2.2. Login Phase

When the user U_i wants to login to the server S_j, the user U_i inserts his/her smart card into a card reader and inputs his/her identity ID_i, password PW_i and the server's identity SID_j. The following steps are:

Step L1. The smart card computes $T_i = V_i \oplus h(ID_i \,||\, h(b \oplus PW_i))$ and $H_i^* = h(T_i)$ and then checks whether $H_i^* = H_i$, If they are equal, U_i proceeds to the next step; Otherwise, the smart card rejects this login request.

Step L2. The smart card generates a nonce N_i and computes $A_i = h(T_i \| h(y) \| N_i)$, $CID_i = h(b \oplus PW_i) \oplus h(T_i \| A_i \| N_i)$, $P_{ij} = T_i \oplus h(h(y) \| N_i \| SID_j)$, $Q_i = h(B_i \| A_i \| N_i)$.

Step L3. $U_i \to S_j :$ CID_i, P_{ij}, Q_i, N_i .

2.3. Verification Phase

Upon receiving the login request message $\{CID_i, P_{ij}, Q_i, N_i\}$, S_j proceeds the following steps to verify the login requester.

Step V1. S_j computes $T_i = P_{ij} \oplus h(h(y) \| N_i \| SID_j)$, $A_i = h(T_i \| h(y) \| N_i)$, $h(b \oplus PW_i) = CID_i \oplus h(T_i \| A_i \| N_i)$ and $B_i = h(h(b \oplus PW_i) \| h(x \| y))$.

Step V2. S_j computes $h(B_i \| A_i \| N_i)$. and checks it with Q_i . If they are equal, S_j generates a nonce N_j to computes $M'_{ij} = h(B_i \| N_i \| A_i \| SID_j)$ and sends $\{M'_{ij}, N_j\}$ to U_i ; Otherwise, S_j terminates the session.

Step V3. Upon receiving $\{M'_{ij}, N_j\}$, U_i computes $h(B_i \| N_i \| A_i \| SID_j)$ and checks it with M'_{ij}. If they are equal, U_i computes $M''_{ij} = h(B_i \| N_j \| A_i \| SID_j)$ and sends back it to S_j ; Otherwise, S_j terminates the session.

Step V4. When receiving $\{M''_{ij}\}$, S_j computes $h(B_i \| N_j \| A_i \| SID_j)$ and checks it with $\{M''_{ij}\}$, If they are equal, U_i passes the authentication of S_j; Otherwise, U_i terminates the session. Finally, U_i and S_j computes $SK = h(B_i \| N_i \| N_j \| A_i \| SID_j)$ as the session key.

2.4. Password Change Phase

When the user U_i wants to change his/her password, the following steps he/she can conduct:

Step P1. The user U_i inserts his/her smart card into a card reader and inputs ID_i, PW_i .

Step P2. The smart card computes $T_i = V_i \oplus h(ID_i \| h(b \oplus PW_i))$ and $H^*_i = h(T_i)$ and then checks whether $H^*_i = H_i$. If they are equal, U_i selects a new password PW_{new} and a new random number b_{new} , and then computes $h(b_{new} \oplus PW_{new})$ and . $V_{new} = T_i \oplus h(ID_i \| h(b_{new} \oplus PW_{new}))$. Finally, U_i sends ID_i and $h(b_{new} \oplus PW_{new})$ to RC over a secure channel.

Step P3. RC computes $B_{new} = h(h(b_{new} \oplus PW_{new}) \| h(x \| y))$, and sends back B_{new} to U_i .

Step P4. The smart card replaces V_i and B_i with V_{new} and B_{new} respectively.

3. Cryptanalysis of Lee-Lin-Chang's Scheme

In this section, we will show that Lee-Lin-Chang's scheme is vulnerable to smart card stolen attack and malicious server attack. Besides, their scheme has the weakness of low efficiency and inconveniency in password change phase.

3.1. Smart Card Stolen Attack

In Lee-Lin-Chang's scheme security analysis, they claimed that an adversary cannot forge a login request to fool S_j, even if the smart card was stolen and the information was extracted by the adversary. However, we find the actual situation is not the case. When an attacker extracted the information $\{V_i, B_i, H_i, b, h(\cdot), h(y)\}$ from U_i's stolen smart card and eavesdropped a previously valid login message $\{CID_i, P_{ij}, Q_i, N_i\}$, he/she can compute $T_i = P_{ij} \oplus h(h(y) \| N_i \| SID_j)$, $A_i = h(T_i \| h(y) \| N_i)$, $h(b \oplus PW_i) = CID_i \oplus h(T_i \| A_i \| N_i)$ With these information, the attacker can initiate replay attack, impersonation attack and off-line password guessing attack as follows.

3.1.1. Replay Attack: If the attacker replays a eavesdropped previously valid login message $\{CID_i, P_{ij}, Q_i, N_i\}$ to S_j, it will pass S_j's verification as the login message is itself valid. Then, S_j will send back message $\{M'_{ij}, N_j\}$ according to Lee-Lin-Chang's scheme. When the attacker receives the message $\{M'_{ij}, N_j\}$, he/she can correctly compute $M''_{ij} = h(B_i \| N_j \| A_i \| SID_j)$ and $SK = h(B_i \| N_i \| N_j \| A_i \| SID_j)$ with the knowledge B_i and A_i. Eventually, the replay attack succeeds.

3.1.2. Impersonation Attack: With the information $T_i, h(b \oplus PW_i), B_i, h(y)$ and SID_j, an attacker can generate a random number N_a, and forge a valid login message $\{CID_i', P'_{ij}, Q_i', N_a\}$ as follows: $A_i' = h(T_i \| h(y) \| N_a), CID'_i = h(b \oplus PW_i) \oplus h(T_i \| A_i' \| N_a)$, $P'_{ij} = T_i \oplus h(h(y) \| N_a \| SID_j)$, $Q_i' = h(B_i \| A_i' \| N_a)$. As shown in replay attack, it is not difficult to see the forged login message $\{CID_i', P'_{ij}, Q_i', N_a\}$ can pass the server provider S_j's verification. Then, the attacker can also correctly agree on a session key SK' with S_j. So, Lee-Lin-Chang's scheme cannot resist impersonation attack as they claimed.

3.1.3. Off-line Dictionary Attack: With the knowledge b and $h(b \oplus PW_i)$, an adversary can process off-line password guessing attack. After obtaining PW_i, he/she can further guess the ID_i with the value $h(ID_i \| h(b \oplus PW_i))$computed from V_i and T_i which he/she has obtained. As such, the attacker has the same privilege as legal user U_i. He/She can do everything U_i can do.

3.2. Malicious Server Attack

In Lee-Lin-Chang's scheme, all system servers and registration center RC share the same secret keys $h(x \| y)$ and $h(y)$. It enables service providing server S_j to masquerade as other service providing servers in the real network environment. Besides, the malicious server S_j can also impersonate the legal user U_i to login other server S_k. If S_j has received a valid login request message $\left\{CID_i, P_{ij}, Q_i, N_i\right\}$ (or intercepted such a message $\left\{CID_i^*, P_{il}^*, Q_i^*, N^*{}_i\right\}$ which was originally sent to server S_l), he/she can computes $T_i = P_{ij} \oplus h(h(y) \| N_i \| SID_j)$, $A_i = h(T_i \| h(y) \| N_i)$, $h(b \oplus PW_i) = CID_i \oplus h(T_i \| A_i \| N_i)$ and $B_i = h(h(b \oplus PW_i) \| h(x \| y))$ (or $T_i = P_{ij}^* \oplus h(h(y) \| N_i^* \| SID_l)$, $A_i^* = h(T_i \| h(y) \| N_i^*)$, $h(b \oplus PW_i) = CID_i^* \oplus h(T_i \| A_i^* \| N_i^*)$ and $B_i = h(h(b \oplus PW_i) \| h(x \| y))$ With the values $T_i, h(y), h(b \oplus PW_i), B_i$ and SID_k, the server S_j can successfully forge a valid login request message as shown in stolen smart card attack above. Therefore, Lee-Lin-Chang's scheme cannot resist the malicious server attack.

3.3. Weakness of Low Efficiency and Inconveniency in Password change Phase

In password change phase of Lee-Lin-Chang's scheme, a user has to exchange some important and highly secret messages with register center RC. On one hand, this inevitably causes some additional delay and consequently decreases the scheme's efficiency. On the other hand, a secure channel is needed when exchanging these highly secret messages. This is inconvenient since users cannot change their password anytime in any place.

4. Our Proposed Scheme

In this section, we propose an improved scheme that is free from all the attacks and weakness mentioned above. There are also three entities in our scheme, *i.e.* the user(U_i), the service providing server S_j and the registration center (RC). RC is assumed to be trusted and responsible for registration and authentication of the U_i and S_j. Registration center(RC) chooses the master key x and a secret number y which only RC knows. Each service providing server S_j needs to register himself/herself with RC using the corresponding identity SID_j. In the registration phase, the registration center (RC) computes $h(SID_j \| y)$ and $h(x \oplus y)$, and then shares $h(x \oplus y)$ with S_j and submits $h(SID_j \| y)$ to S_j through a secure channel. The proposed scheme also consists four phases: the registration phase, the login phase, the authentication and session key agreement phase, and the password change phase. The login and the authentication with session key agreement phases are summarized in Figure 2.

4.1. Registration Phase

When the user U_i wants to access the systems, the steps of the registration phase are as follows.

Step R1. $U_i \Rightarrow RC$: SID_i . U_i freely selects his/her identity ID_i and password PW_i . Then U_i sends ID_i to the registration center RC over a secure channel.

Step R2. RC computes $\mathrm{T}_i = h(h(ID_i \| b_i) \| x)$ and $\mathrm{B}_i = h(T_i \| h(x \| y))$, where b_i is a random number generated by RC for the user U_i and only used once.

Step R3. $RC \Rightarrow U_i$: Smart Card. RC stores $\{T_i, B_i, h(\cdot)\}$ in a smart card, and issues the card to U_i over a secure channel.

Step R4. U_i inputs ID_i , PW_i to the issued smart card. The smart card computes $V_i = h(ID_i \| PW_i)$ and $R_i = B_i \oplus h(PW_i \oplus ID_i)$, then stores V_i and substitutes B_i with R_i. Eventually, the smart card contains $\{T_i, V_i, R_i, h(\cdot)\}$.

4.2. Login Phase

This phase is invoked whenever the user U_i wants to access the resources of the service provider S_j . The steps are as follows:

Step L1. U_i inserts his/her smart card into the smart card reader and inputs his/her identity $ID^*{}_i$, password $PW^*{}_i$ .Then the smart card computes $V^*{}_i = h(ID_i^* \| PW^*{}_i)$ and checks whether $V^*{}_i = V_i$. If they are equal, it means U_i is a legal user; Otherwise, the smart card rejects this login request.

Step L2. After verification, the smart card generates a random number N_{i1} , and computes $B_i = R_i \oplus h(PW_i \oplus ID_i),\ CID_i = h(B_i \| N_{i1}) \oplus (ID_i \| B_i)$ and $Q_{ij} = h(ID_i \| B_i \| N_{i1} \| SID_j)$.

Step L3. $U_i \to S_j$: $\{CID_i, T_i, Q_{ij}, N_{i1}\}$.

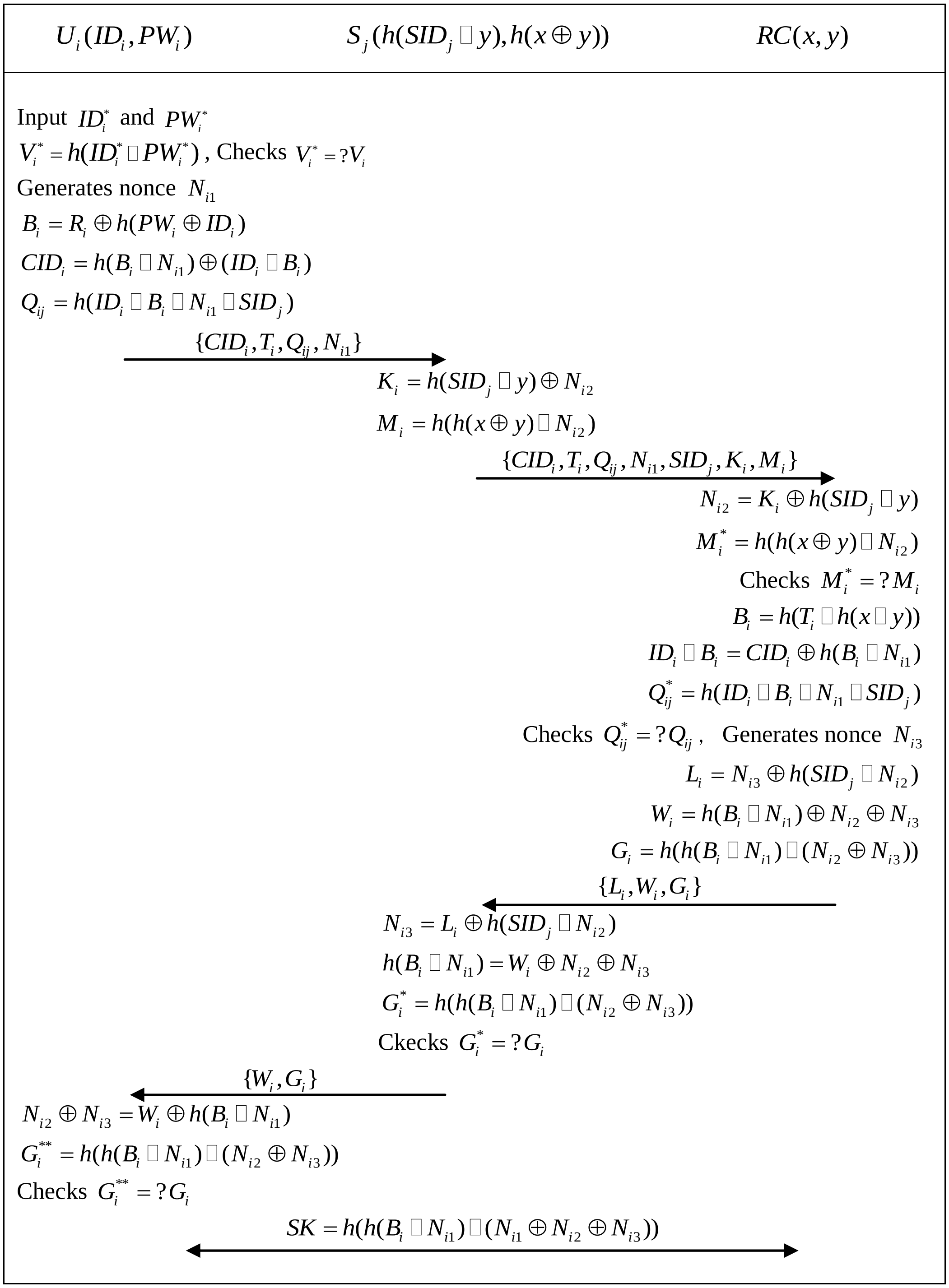
4.3. Authentication and Session Key Agreement Phase

Upon receiving the login request message $\{CID_i, T_i, Q_{ij}, N_{i1}\}$, the service provider S_j Authenticates the user U_i with the following steps:

Step V1. the server S_j generates a nonce N_{i2} , and computes $K_i = h(SID_j \square y) \oplus N_{i2}$ and $M_i = h(h(x \oplus y) \square N_{i2})$.

Step V2. $S_j \to RC$: $\{CID_i, T_i, Q_{ij}, N_{i1}, SID_j, K_i, M_i\}$.

Step V3. After receiving the login request message $\{CID_i, T_i, Q_{ij}, N_{i1}, SID_j, K_i, M_i\}$, RC computes $N_{i2} = K_i \oplus h(SID_j \square y)$, $M_i^* = h(h(x \oplus y) \square N_{i2})$, and checks whether $M_i^* = M_i$. If



$U_i(ID_i, PW_i)$ $S_j(h(SID_j \| y), h(x \oplus y))$ $RC(x, y)$

Input ID_i^* and PW_i^*

$V_i^* = h(ID_i^* \| PW_i^*)$, Checks $V_i^* = ?V_i$

Generates nonce N_{i1}

$B_i = R_i \oplus h(PW_i \oplus ID_i)$

$CID_i = h(B_i \| N_{i1}) \oplus (ID_i \| B_i)$

$Q_{ij} = h(ID_i \| B_i \| N_{i1} \| SID_j)$

$\{CID_i, T_i, Q_{ij}, N_{i1}\}$

$K_i = h(SID_j \| y) \oplus N_{i2}$

$M_i = h(h(x \oplus y) \| N_{i2})$

$\{CID_i, T_i, Q_{ij}, N_{i1}, SID_j, K_i, M_i\}$

$N_{i2} = K_i \oplus h(SID_j \| y)$

$M_i^* = h(h(x \oplus y) \| N_{i2})$

Checks $M_i^* = ?M_i$

$B_i = h(T_i \| h(x \| y))$

$ID_i \| B_i = CID_i \oplus h(B_i \| N_{i1})$

$Q_{ij}^* = h(ID_i \| B_i \| N_{i1} \| SID_j)$

Checks $Q_{ij}^* = ?Q_{ij}$, Generates nonce N_{i3}

$L_i = N_{i3} \oplus h(SID_j \| N_{i2})$

$W_i = h(B_i \| N_{i1}) \oplus N_{i2} \oplus N_{i3}$

$G_i = h(h(B_i \| N_{i1}) \| (N_{i2} \oplus N_{i3}))$

$\{L_i, W_i, G_i\}$

$N_{i3} = L_i \oplus h(SID_j \| N_{i2})$

$h(B_i \| N_{i1}) = W_i \oplus N_{i2} \oplus N_{i3}$

$G_i^* = h(h(B_i \| N_{i1}) \| (N_{i2} \oplus N_{i3}))$

Ckecks $G_i^* = ?G_i$

$\{W_i, G_i\}$

$N_{i2} \oplus N_{i3} = W_i \oplus h(B_i \| N_{i1})$

$G_i^{**} = h(h(B_i \| N_{i1}) \| (N_{i2} \oplus N_{i3}))$

Checks $G_i^{**} = ?G_i$

$SK = h(h(B_i \| N_{i1}) \| (N_{i1} \oplus N_{i2} \oplus N_{i3}))$

Figure 2. The Proposed Scheme

they are equal, the validity of the server S_j is verified by RC; Otherwise, the RC terminates the session.

Step V4. RC computes $B_i = h(T_i \| h(x \| y))$, $ID_i \| B_i = CID_i \oplus h(B_i \| N_{i1})$, $Q_{ij}^* = h(ID_i \| B_i \| N_{i1} \| SID_j)$ and checks whether $Q_{ij}^* = Q_{ij}$. If they are equal, the validity of the user U_i is verified by RC ; Otherwise, RC rejects the login request.

Step V5. RC generates a nonce N_{i3} , and computes $L_i = N_{i3} \oplus h(SID_j \| N_{i2})$, $W_i = h(B_i \| N_{i1}) \oplus N_{i2} \oplus N_{i3}$ and $G_i = h(h(B_i \| N_{i1}) \| (N_{i2} \oplus N_{i3}))$.

Step V6. $RC \rightarrow S_j$: $\{L_i, W_i, G_i\}$.

Step V7. Upon receiving $\{L_i, W_i, G_i\}$, S_j computes $N_{i3} = L_i \oplus h(SID_j \| N_{i2})$, $h(B_i \| N_{i1}) = W_i \oplus N_{i2} \oplus N_{i3}$, $G_i^* = h(h(B_i \| N_{i1}) \| (N_{i2} \oplus N_{i3}))$ and checks whether $G_i^* = G_i$. If they are equal, it means RC is the legal registration center; Otherwise, S_j terminates the session.

Step V8. $S_j \rightarrow U_i$: $\{W_i, G_i\}$.

Step V9. Upon receiving $\{W_i, G_i\}$, U_i computes $N_{i2} \oplus N_{i3} = W_i \oplus h(B_i \| N_{i1})$, $G_i^{**} = h(h(B_i \| N_{i1}) \| (N_{i2} \oplus N_{i3}))$ and checks whether $G_i^{**} = G_i$. If they are equal, RC and S_j are verified by U_i ; Otherwise, U_i terminates the session.

Step V10. The user U_i , the server S_j and the registration center RC agree on a common session key $SK = h(h(B_i \| N_{i1}) \| (N_{i1} \oplus N_{i2} \oplus N_{i3}))$.

4.4. Password Change Phase

This phase is invoked whenever U_i wants to change his/her password PW_i without the help of RC . The steps are as follows:

Step P1. U_i inserts his smart card into the smart card reader, then enters ID_i^* , PW_i^* and requests to change password.

Step P2. U_i 's smart card computes $V_i^* = h(ID_i^* \| PW_i^*)$ and checks whether V_i^* and V_i is equal or not. If not, the smart card rejects the password change request; Otherwise, U_i selects a new password PW_{new} .

Step P3. U_i 's smart card computes $V_{new} = h(ID_i^* \| PW_{new})$, $R_{new} = R_i \oplus h(PW_i^* \oplus ID_i^*) \oplus h(PW_{new} \oplus ID_i^*)$ and substitutes V_i , R_i with V_{new} , R_{new} respectively.

5. Security Analysis

In this section, we will mainly discuss the enhanced security and efficiency of our improved scheme. The other security features are the same as Lee-Lin-Change's scheme.

5.1. Stolen Smart Card Attack

If the user U_i 's smart card has been lost or stolen, the adversary obtained the card can extract the information $\{T_i, V_i, R_i, h(\cdot)\}$ stored in the smart card. With these information, it is impossible for adversary to get any useful value (such as x, y, ID_i, PW_i or B_i) to forge a valid login request message. Even if a previously valid login request message $\{CID_i, T_i, Q_{ij}, N_{i1}\}$ was eavesdropped or intercepted by the adversary, he/she cannot initiate replay or impersonation attack since B_i is computed in no way from $\{T_i, V_i, R_i, h(\cdot)\}$ and $\{CID_i, T_i, Q_{ij}, N_{i1}\}$. So, our proposed scheme is secure against stolen smart card attack.

5.2. Off-Line Dictionary Attack

In this attack, the adversary can record messages and attempts to guess user U_i's identity ID_i or password PW_i from the recorded messages. Because of the low entropy of ID_i and PW_i selected freely by user U_i himself/herself, we assume that an adversary is able to guess ID_i or PW_i independently. However, as pointed out by Sood, Sarje and Singh [19], it is not possible to guess the two parameters correctly at the same time in real polynomial time. In our proposed scheme, an adversary might obtain values $V_i = h(ID_i \| PW_i)$, $R_i = B_i \oplus h(PW_i \oplus ID_i)$, $\mathrm{T}_i = h(h(ID_i \| b_i) \| x)$, $CID_i = h(B_i \| N_{i1}) \oplus (ID_i \| B_i)$ and $Q_{ij} = h(ID_i \| B_i \| N_{i1} \| SID_j)$ through various methods, such as stealing the smart card, eavesdropping or intercepting previously valid login request messages. He/She cannot guess ID_i or PW_i from V_i since he is unable to guess the two parameters simultaneously. Furthermore, the adversary also cannot guess ID_i or PW_i from T_i, R_i, CID_i or Q_{ij} without the knowledge x, b_i and B_i. Therefore, the proposed scheme is secure against off-line dictionary attack.

5.3. Malicious user attack

A malicious privileged user U_i with knowledge ID_i and PW_i also can extract the information $\{T_i, V_i, R_i, h(\cdot)\}$ stored in his/her own smart card. In our proposed scheme, the malicious privileged user cannot get useful information (such as $x, y, B_k, h(x \square y), h(SID_j \square y)$ or $h(x \oplus y)$) to impersonate other user U_k to login the system or masquerade as a server S_j to fool users. Therefore, the proposed scheme can resist the malicious user attack.

5.4. Malicious Server Attack

Since every server has his/her own secret key $h(SID_j \square y)$ and has no way to compute other's secret key $h(SID_k \square y)$ without the value y, a malicious server S_j cannot masquerade as other server S_k to fool users. In addition, even if a previously valid login request $\{CID_i, T_i, Q_{ij}, N_{i1}\}$ is eavesdropped, the malicious server cannot forge a valid login message $\{CID_i^{'}, T_i^{'}, Q_{ij}^{'}, N_{i1}^{'}\}$ to login other server S_k masquerading U_i because he/she cannot get secret B_i. Consequently, our scheme is secure against malicious server attack.

5.5. User's Anonymity

In the registration phase of our proposed scheme, the secure channel and a random number b_i generated by RC are used to protect the user's identity from disclosure. In the login phase, the user U_i submits the masked identity $CID_i = h(B_i \| N_{i1}) \oplus (ID_i \| B_i)$ instead of the real identity ID_i in his/her login request message. The authentication and session key agreement of the proposed scheme is based on computation of the secret information B_i, but not the real identity ID_i. Based on the above analysis, we can say that our proposed protocol can provide the user's anonymity.

In fact, the user's anonymity can be classified into transmission anonymity and login anonymity, depending on whether the real identity ID_i can be recovered or not from the dynamic identity CID_i in authentication phase. The main difference between these two cases is that the former has the feature that the user U_i can be traced and prevented from sabotaging by RC, while the latter has not. In some applications which favour this feature, the transmission anonymity is preferable. In some other applications which require to avoid the feature to the greatest extent, the login anonymity will be more suitable. To the best of our knowledge, most of the dynamic identity based schemes previously proposed belong to the case of login anonymity. Here, Our proposed scheme belongs to the case of transmission anonymity since the real identify ID_i can be easily recovered by RC from B_i and $ID_i \Box B_i$ computed in the authentication process. In addition, just for a little modification, our scheme will be changed to the case of login anonymity. In the login phase, the U_i 's card generates another nonce $N_{i1}^{'}$ and computes $CID_i = h(B_i \| N_{i1}) \oplus N_{i1}^{'}$, $Q_{ij} = h(B_i \| N_{i1} \| SID_j \Box N_{i1}^{'})$ instead of $CID_i = h(B_i \| N_{i1}) \oplus (ID_i \| B_i)$, $Q_{ij} = h(ID_i \| B_i \| N_{i1} \| SID_j)$. Correspondingly, RC computes $N_{i1}^{'} = CID_i \oplus h(B_i \| N_{i1})$, $Q_{ij}^{*} = h(B_i \| N_{i1} \| SID_j \Box N_{i1}^{'})$ rather than $(ID_i \| B_i) = CID_i \oplus h(B_i \| N_{i1})$, $Q_{ij}^{*} = h(ID_i \| B_i \| N_{i1} \| SID_j)$ in the authentication phase. All other processes remain unchanged. It is not difficult to see that the modified scheme is login anonymous. Therefore, our proposed scheme is more flexible for applications.

5.6. Efficiency and Conveniency in Password Change Phase

In our scheme, when user U_i wants to change his/her password, the user U_i can finish it by himself/herself without the help of RC. Naturally, there is no need to exchange any secret information between the users and RC. Therefore, the efficiency in password change phase of our scheme is improved. Besides, since no secret information is exchanged, the user U_i can be more convenient and secure to change his/her password offline, instead of setting up secure channel firstly between the user and registration center as shown in Lee-Lin-Chang's scheme.

6. Cost and Functionality Analysis

In this section, we evaluate the computation cost and functionality of our proposed scheme through comparing with several recently proposed schemes. To analyze the computational complexity of these schemes, we define the notation T_h as the time complexity for hash function. Since exclusion-OR and concatenation operations require very few computation, they are usually neglected considering its computation cost.

In Table 2, we compare the performance of our proposed scheme and those five related schemes. Since login and authentication phases are the principle parts of an remote authentication scheme and should be implemented for each session, we mainly consider the computation cost of these two phases as shown in almost performance analysis of related works.

Table 2. Cost Comparisons of our Scheme and Previously Proposed Schemes

	Login phase	Verification phase	Total
Proposed protocol	$4T_h$	$13T_h$, $1T_s$	$17T_h$
Li et al. [15]	$7T_h$	$21T_h$	$28T_h$
Sood et al. [21]	$7T_h$	$18T_h$	$25T_h$
Hsiang-Shih [4]	$7T_h$	$17T_h$	$24T_h$
Lee-Lin-Chang [10]	$7T_h$	$11T_h$	$18T_h$
Liao-Wang [16]	$6T_h$	$9T_h$	$15T_h$

The first four schemes listed in Table 2 share a common feature that the register center(RC) or the control server(CS) plays a part in authentication process. The participation in authentication of RC or CS avoids malicious servers to masquerade as other servers to fool the legal users. On the contrary, the last two schemes cannot resist the malicious server attack without this mechanism, although these two schemes save computation cost of few hash operations generally. From Table 2, it is obvious that our proposed scheme is most efficient among the first four schemes with the mechanism mentioned above. Even comparing with Lee-Lin-Chang's scheme [10], the proposed scheme requires one less hash operation. Therefore, our proposed scheme is more efficient.

Table 3. Functionality Comparisons of our Scheme and Previously Proposed Schemes

	Ours	Lee-Lin-Chang (2011)	Li et al. (2011)	Sood et al. (2011)	Hsiang-Shih (2009)	Liao-Wang (2009)
User's anonymity	Yes	Yes	Yes	Yes	Yes	Yes
Computation cost	Low	Low	Low	Low	Low	Low
Single registration	Yes	Yes	Yes	Yes	Yes	Yes
Resist stolen smart card attack	Yes	No	Yes	No	No	No
Resist malicious user attack	Yes	Yes	No	No	No	No
Resist malicious server attack	Yes	No	Yes	Yes	No	No
Password change without the help of RC or CS	Yes	No	Yes	Yes	Yes	Yes

Table 3 lists the functionality comparison among those six schemes. It can be clearly seen that our scheme is more secure against various attacks than other five related schemes.

7. Conclusions

In this paper, we prove that Lee-Lin-Chang's dynamic ID based multi-server remote user authentication scheme is vulnerable to smart card stolen attack and malicious server attack, and show it is not efficient enough and not convenient to users in password change phase. Then we proposed an improved dynamic ID based scheme to remedy these weaknesses without losing security features. To avoid smart card stolen attack, the security of our scheme is based only on the secure keys owned by users, servers and registration center and a secure one-way hash function. Consequently, there is no useful information can be computed from the values stored in smart cards in the proposed scheme. To avoid malicious server attack, we move the user authentication process from service providing servers to the registration center and ensure each server has a different secret key $h(SID_j \square y)$. Through comparing with several schemes proposed recently, we demonstrated our proposed scheme is more secure and efficient. Therefore, the proposed scheme is more suitable for applications with high security requirements.

Acknowledgements

This work was partially supported by the Doctoral Fund of University of Jinan (Granted No. XBS0835), and the project of Jinan City Science and Technology Program (Granted No. 201202014).

References

[1] C. C. Chang and J. S. Lee, “An efficient and secure multi-server password authentication scheme using smart cards”, Proceedings of the third international conference on cyberworlds, **(2004)**, pp. 417-22.

[2] C. I. Fan, Y. C. Chan and Z. K. Zhang, “Robust remote authentication scheme with smart cards”, Computers & Security, vol. 24, **(2005)**, pp. 619-28.

[3] W. W. Han, “Weaknesses of a dynamic identity based authentication protocol for multi-server architecture”, Arxiv preprint, arXiv: 1201.0883, **(2012)**.

[4] H. C. Hsiang and W. K. Shih, “Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment”, Computer Standards & Interfaces, vol. 31, **(2009)**, pp. 1118-1123.

[5] W. S. Juang, “Efficient multi-server password authenticated key agreement using smart cards”, IEEE Transaction on Consumer Electronics, vol. 50, **(2004)**, pp. 251-255.

[6] J. Y. Kim, H. K. Choi and J. A. Copeland, “Further improved remote user authentication scheme”, IEICE Transaction on Fundamentals, E94-A, **(2011)**, pp. 1426-1433.

[7] S. K. Kim and M. G. Chung, “More secure remote user authentication scheme”, Computer Communications, vol. 32, **(2009)**, pp. 1018-1021.

[8] W. C. Ku and S. M. Chen, “Weakness and improvements of an efficient password based remote user authentication scheme using smart cards”, IEEE Transaction on Consumer Electronics, vol. 50, **(2004)**, pp. 204-207.

[9] L. Lamport, “Password authentication with insecure communication”, Communications of the ACM, vol. 24, **(1981)**, pp. 770-772.

[10] C. C. Lee, T. H. Lin and R. X. Chang, “A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards”, Expert Systems with Applications, vol. 38, **(2011)**, pp. 13863-13870.

[11] S. W. Lee, H. S. Kim and K. L. Yoo, “Efficient nonce-based remote user authentication scheme using smart cards”, Applied Mathematics and Computation, vol. 167, **(2005)**, pp. 355-361.

[12] W. B. Lee and C. C. Chang, “User identification and key distribution maintaining anonymity for distributed computer network”, International Journal of Computer Systems Science & Engineering, vol. 15, **(2000)**, pp. 211-214.

[13] C. T. Li and M. S. Hwang, “An efficient biometrics-based remote user authentication scheme using smart cards”, Journal of Network and Computer Applications, vol. 33, **(2010)**, pp. 1-5.

[14] L. H. Li, L. C. Lin and M. S. Hwang, “A remote password authentication scheme for multi-server architecture using neural networks”, IEEE Transactions on Neural Networks, vol. 12, **(2001)**, pp. 1498-1504.

[15] X. Li, Y. P. Xiong, J. Ma and W. D. Wang, “An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards”, Journal of Network and Computer Applications, vol. 35, **(2012)**, pp. 763-769.

[16] Y. P. Liao and S. S. Wang, “A secure dynamic ID based remote user authentication scheme for multi-server environment”, Computer Standards & Interfaces, vol. 31, **(2009)**, pp. 24-29.

[17] J. Y. Liu, A. M. Zhou and M. X. Gao, “A new mutual authentication scheme based on nonce and smart cards”, Computer Communications, vol. 31, **(2008)**, pp. 2205-2209.

[18] I. C. Lin, M. S. Hwang and L. H. Li, “A new remote user authentication scheme for multi-server architecture”, Future Generation Computer Systems, vol. 1, **(2003)**, pp. 13-22.

[19] J. J. Shen, C. W. Lin and M. S. Hwang, “A modified remote user authentication scheme using smart cards”, IEEE Transaction on Consumer Electronics, vol. 49, **(2003)**, pp. 414-416.

[20] R. G. Song, “Advanced smart card based password authentication protocol”, Computer Standards & Interfaces, vol. 32, **(2010)**, pp. 321-325.

[21] S. K. Sood, A. K. Sarje and K. Singh, “A secure dynamic identity based authentication protocol for multi-server architecture”, Journal of Network and Computer Applications, vol. 34, **(2011)**, pp. 609-618.

[22] T. S. Wu and C. L. Hsu, “Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks”, Computer & Security, vol. 23, **(2004)**, pp. 120-125.