World Applied Sciences Journal 15 (6): 799-805, 2011
ISSN 1818-4952

A New Secure Mutual User Identification Scheme Based on ID-Based Cryptosystem

[1]S.H Sajjadijahromi, [2]M.H Mehrabanjahromi and [3]M. Zareianjahromi

[1]Islamic Azad University, Neyriz Branch, Iran
[2]Islamic Azad University, Neyriz Branch, Iran
[3]Department of Electrical and Computer Engineering,
Kerman Graduate University of Technology, Kerman, Iran

Abstract: Most of identification schemes based on identity that discussed up to now are performed in one direction. In these schemes only one side of communicational parties can introduce itself to observe but other side could not be sure that other user is legitimate or not. Therefore, one of our goals in this paper is to propose a secure mutual identification scheme based on identity, as communicational parties that can prove themselves to each other. The second goal in our scheme is to provide an efficient method for using in wireless environment where limited resources in terms of energy. We compare our scheme with two schemes that recently proposed in term of computational complexities and communication cost.our simulation results show that our proposed scheme is real secure mutual identification scheme and we can use it in wireless environment.

Key words: Mutual Identification · Timestamps · Trusted Authority · Base Station

INTRODUCTION

Since the idea of ID-Based cryptosystem was first introduced in 1984 by Shamir [1], there have been many studies focus on various kinds of this system as ID-Based cryptosystem, ID-Based signature scheme and ID-Based key distribution systems [2-7]. In 1998 Tseng and Jan proposed a user identification scheme based on an identity-Based non interactive public key distribution system [8]. In which a user can prove his identity to another person without revealing his secret key, but this scheme uses a three passes protocol which is not suitable for application in a wireless environment. Therefore, Hwang *et al*. improve Tseng and Jan's scheme to be more suitable for application in a wireless environment [9]. In 2006, Chou *et al*. presented a forgery attack to Hwang *et al*. scheme and then proposed a secure one-way identification scheme to improvement this weakness [10]. This paper suggest a mutual identification scheme that hold security feature of previous schemes whereas base station and mobile device can trust to each other legally while it will be usable in the wireless network.

The reminder of this paper is organized as follows. Section 2, reviews the Hwang *et al*. Section 3, shows that Hwang *et al*.'s scheme is not secure against the key forgery attack and how an adversary can perform the attack successfully. Section 4, briefly reviews Chou *et al*.'s user identification scheme. Section 5, presents the proposed scheme. Section 6, analyze the security of proposed scheme. In section 7, the performance analyzes is discussed. Section 8, simulated our scheme within the MATLAB framework. Finally, we give the conclusions.

Review of Hwang *et Al*.'S Scheme: Three kinds of entities are involved in the scheme: a trusted authority (TA), mobile device (M) and base station (BS). The TA is responsible for initializing the system parameters and assigning a secret key to each registered user.

The identification scheme consists of three phase: the initialization phase, user registration phase and user identification phase. Descriptions of these phases are given below.

Initiation Phase: For system setup, TA is used to generate system parameters. TA chooses four primes p_j between 60 and 70 decimal digits, where for each p_j

Corresponding Author: S.H. Sajjadijahromi, Islamic Azad University, Neyriz Branch, Iran.
P.O. Box 74179-34367, Iran, Jahrom. Tel/Fax: +98 9177920700.

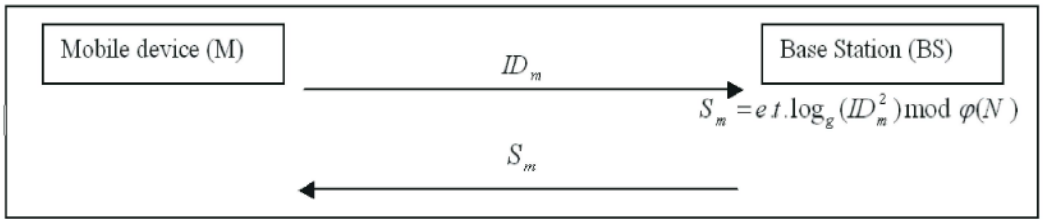

Fig. 1: User registration phase of the Hwang *et al*. scheme.

such that the numbers $(p_j - 1)/2$ are odd and pair-wise relatively prime. Let $N = p_1.p_2.p_3.p_4$. The TA also selects an integer $]\backslash e$ in $Z^*_{\varphi(N)}$ and computes the secret value d which satisfies $e.d \equiv 1 \bmod \varphi(N)$ and $h(.)$ is a one-way hash function. Finally, TA chooses a random integer t from $Z^*_{\varphi(N)}$.

User Registration Phase: When M joins the system, the procedure of user registration phase is shown as follows (as depicted in Fig. 1).

Step 1: The M presents his or her unique identity ID_m to the TA.

Step 2: The TA then computes:

$$S_m = e.t.\log_g(ID_m^2) \bmod \varphi(N) \quad (1)$$

$$v = t^{-1} \bmod \varphi(N) \quad (2)$$

And sends S_m to M as his or her secret key.

Finally, the trusted authority publishes $\{N, g, e, h(.)\}$ and keeps $\{p_1,p_2,p_3,p_4,t,v,d\}$ secret for all user and user M publishes $\{ID_m\}$ and keeps $\{ID_m\}$ secretly.

User Identification Phase: Suppose that the M wants to show its identity is legal to the BS. They perform the protocol as follows:

Step 1: M chooses a random integer $k \in_R Z_N^*$ and computes Y and Z as follows:

$$Y = (ID_m^2)^k \bmod N \quad (3)$$

$$Z = (ID_b^2)^{k.s_m.T} \bmod N \quad (4)$$

Where, T is a timestamps. Then, TA sends $L = \{(ID_m \| Y \| Z), T\}$ to BS.

Step 2: After receiving the above message from M, BS computes $Z' = Y^{sbT} \bmod N$. Where S_b is BS's secret key.

Step 3: BS checks the equation $Z \overset{?}{=} Z'$. If the equation holds, BS will confirm that M's identity is a valid.

Forgery Attack on Hwang *et al*.'S Scheme: In Hwang *et al*.'s scheme, an attacker can easily impersonate the M. Suppose a malicious user (H) wants to impersonate a legal user M following the Hwang's protocol. We can easily indicate how he can succeed in the forgery attack as follows:

Step 1: User H intercepts the transmitted message $L = \{(ID_m \| Y \| Z), T\}$ and create another timestamps T'.

Step 2: User H replaces the intercepted message components Y with Y' and Z with Z'. Where $Y' = (Y^{sh.T'}) \bmod N$ and $Z' = (Z^{sh.T'}) \bmod N$. He can replace ID_m with his own ID, ID_h. Where S_h is an H's secret key.

Step 3: After receiving message L' from H, BS computes:

$$Z'' = (Y')^{Sh.T'} \bmod N \quad (5)$$

Step 4: BS checks whether the equation $Z' \overset{?}{=} Z''$ holds, if it holds, BS will assure that H's identity is valid. After that, according to the protocol proposed by Hwang *et al*., H can easily impersonate as a legal user successfully without being detected by BS. The verification equation $Z' \overset{?}{=} Z''$ can be verified as follows.

$$\begin{cases} Z' = Z^{S_h.T'} \bmod N = [(ID_b^2)^{k.S_m.T}]^{S_h.T'} \bmod N \\ Z'' = (Y')^{S_b.T'} \bmod N = (Y^{S_h.T})^{S_b.T'} \bmod N \Rightarrow \\ Z'' = \{[(ID_m^2)^k]^{S_h.T}\}^{S_b.T'} \bmod N \end{cases} \quad (6)$$

And also we have

$$S_m = e.t.\log_g(ID_m^2) \bmod \varphi(N) \Rightarrow ID_m^2 = g^{S_m.v.d} \quad (7)$$

Therefore, Eq. 8 can obtain from above equations

$$Z'' = (g^{S_m.v.d})^{k.S_h.T.S_b.T} \bmod N = [(ID_b^2)^{k.S_h.T}]^{S_m.T''} \bmod N = Z' \quad (8)$$

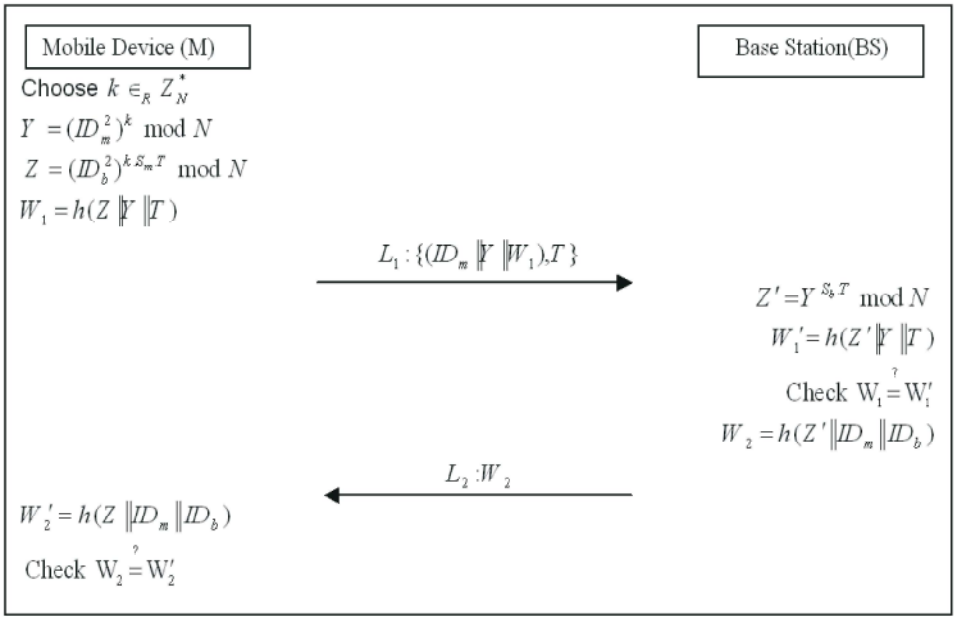

Fig. 2: User identification phase of the proposed scheme.

Therefore, no matter what value of T is, the malicious can always succeed in his forgery attack.

Review of Chou *et al.*'S Scheme: In order to solve the weakness mentioned in Section 3, Chou *et al*. replace the timestamp with a value which is derived from the secret communication key, denoted c shared between the mobile device M and BS.

In fact, their scheme is almost the same as Hwang *et al*.'s scheme except for the value of c. These identification schemes consist of three phases: the initialization phases, user registration phase and user identification phase. System initialization and the user registration phases are same as Hwang *et al*. scheme but with some change that we explained in the following.

When the M joins the system, in addition to the original parameters generated, TA also chooses two large primes p and q, satisfying $4|(p-1)$ and $4|(q-1)$ respectively, then computes $n=p.q$. let the symbol QR_n denote the set of all quadratic residue numbers in [1,n-1]. TA also computes a QR_p and QR_q. Finally, TA sends (n,p,q,QR_p,QR_q) to M in a secure manner.

Each time M wants to indicate his identity ID_m is legal to BS; M chooses a different secret communication key $c \in (Qr_p \cap QR_q)$ and computes $a = c^2 \bmod N$.

The relationship between c and a is one-to-one which is proved in [11], one can uniquely determine c whenever given a fixed value a.

User Identification Phase: Suppose M wishes to identity itself to BS. It follows the steps below.

Step 1: M chooses a random number $k \in_R Z_N^*$ and computes Y and Z as follows

$$Y = (ID_m^2)^k \bmod N \tag{9}$$

$$Z = (ID_b^2)^{k.S_m.c} \bmod N \tag{10}$$

Then, M sends the message $L = \{(ID_m \| Y \| Z), a\}$ to BS.

Step 2: After receiving message L from M, BS determines the value c from a and then, BS computes $Z' = Y^{sb.c} \bmod N$. BS checks whether the equation $Z \stackrel{?}{=} Z'$ holds, if it holds, BS will assure that M's identity is valid.

The verification equation $Z \stackrel{?}{=} Z'$ can be verified as follows.

$$Z' = Y^{S_b.c} \bmod N = (ID_m^2)^{k.S_b.c} \bmod N = (g^{S_m.v.d})^{k.S_b.c} = (ID_b^2)^{k.S_m.c} \bmod N = Z \tag{11}$$

The Proposed Scheme: The proposed scheme's aim to provide a mutual identification scheme based on identity, in which the M and BS can verify each other identities. This scheme is similar to two recent proposed schemes which are consisting of three phases: initialization phase, user registration phase and user identification phase. Initialization and user registration phases are same as

Hwang *et al*. scheme. So, in this paper only describe, identification phase of the proposed scheme.

User Identification Phase: If the M wants to gain the access privilege from the BS, M and BS will cooperatively perform the following steps (as depicted in Fig. 2).

Step 1: M choose a random number $k \in_R Z_N^*$ and computes Y, Z and W_1 as follows

$$Y = (ID_m^2)^k \bmod N \tag{12}$$

$$Z = (ID_b^2)^{k.S_m.T} \bmod N \tag{13}$$

$$W_1 = h(Z\|Y\|T) \tag{14}$$

Where, T is a timestamp. Then, M sends $L_1 = \{(ID_m\|Y\|W_1),T\}$ to BS.

Step 2: Upon, receiving L_1 from M, BS computes Z' and W_1' as follows

$$Z' = Y^{sb.T} \bmod N \tag{15}$$

$$W_1' = h(Z'\|Y\|T) \tag{16}$$

BS check the equation $W_1 \overset{?}{=} W_1'$. If the equation holds, BS will confirm that M's identity is valid; otherwise request is rejected. If successful, BS computes $W_2 = h(Z'\|ID_m\|ID_b)$ and sends $W_2 = h(Z'\|ID_m\|ID_b)$ to M.

Step 3: After receiving message W_2 from BS, M computes $W_2' = h(Z\|ID_m\|ID_b)$. Then checks the equation $W_2 \overset{?}{=} W_2'$. If it holds, M believes that the identity of BS is valid.

Security Analysis: In this section, evaluated the security of our proposed scheme by examining a series of possible attacks-replay attack, impersonation attack and obtain secret key.

The security of the proposed scheme is based on three well-known cryptographic assumptions. Analyses that follow are based on the following assumptions:

Definition 1: One way hash function (OWHF) [12]: let *h(.)* be a one-way cryptography hash function. (i) Given y, it is computationally intractable to find x such that $y = h(x)$; (ii) it is computationally intractable to find $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$.

Definition 2: Factorization (FAC) [13]: Let $N=p.q$ and $\gcd(e, \varphi(N)) = 1$, where p and q are unknown large primes. For any $y \in Z_N^*$, it is computationally infeasible to derive x such that $y = x^e$ with the knowledge of N and e.

Definition 3: Discrete Logarithm Problem over Z_N^* (DLP_N)[12]: Let $N = pq$ and g be a primitive root for both Z_p^* and Z_q^*, where p and q are randomly strong primes. Given $y = g^x \bmod N \in Z_N^*$, it is computationally intractable to derive x.

Since the proposed scheme explicitly uses the current timestamp in generating the authentication data, reply attack is thus prevented.

In the system initiation phase, computing a discrete logarithm modulo prime N without knowing the prime factors of N is still infeasible. It can be shown that computing a discrete logarithm modulo for composite number N is at least as difficult as factoring the modulus. Because the system initiation phase of our scheme is the same as one for the Maurer and Yacobi scheme expect for an increase of one value, the discussion is omitted here. The detailed description can be found in the literature [14].

The attacker have problem for obtain private key S_m with attention secret parameter t and $\varphi(N)$.

The attacker can attempt to modify a message $L_1 = \{(ID_m\|Y\|W_1),T\}$, into $L'_1 = \{(ID_m\|Y'\|W'_1),T\}$ where T' is the attacker's current timestamp. However such modification will fail, because an attacker has no way for obtaining the valid value $Z = (ID_b^2)^{k.S_m.T} \bmod N$ to compute the valid parameter W_1. Furthermore, it is infeasible that an attacker can get Z using $L_1 = \{(ID_m\|Y\|W_1),T\}$, because one-way hash function that we using in our scheme is secure. Thus, the impersonation attack cannot be successful.

Performance Analysis: This section compare the performances of the proposed scheme with the Hwang *et al*. and Chou *et al*. schemes in term of computation complexities and communication cast. The following notations are used to facilitate the performance evaluation:

T_h: The time for executing a one-way hash function.
T_{exp}: The time for executing a modular exponentiation computation.
$|x|$: The bit length of x

Table 1: Performance of the proposed scheme and previously proposed schemes

		Computational Complexity		
	Communication Cost	Mobile Device (M)	Base Station (BS)	Mutual Identification
The Hwang *et al*.[9]	$2\|N\|+\|ID\|+\|T\|$	$6T_{exp}$	$2T_{exp}$	⊠
The Chou *et al*.[10]	$3\|N\|+\|ID\|$	$7T_{exp}$	$6T_{exp}$	⊠
The proposed scheme	$\|N\|+\|ID\|+\|T\|+2\|H\|$	$6T_{exp}+2T_h$	$6T_{exp}+2T_h$	√

Table 2: Radio model parameters

Parameter	Value
ε_s	10 pJ/bit/m2
ε_l	0.0013 pJ/bit/m4
E_e	50 nJ/bit
E_{BF}	5 nJ/bit
L	4000 bit

Table 3: Simulated network parameters

Parameter	Value
Number of nodes	500
Network size	50*50 m^2
Base Station	(100,25) m
Initial energy of nodes	2 j
Min energy of nods	0.001 j
Data transfer rate	bandwidth= 1 Mbps

The comparisons between the proposed scheme and Hwang *et al*. and Chou *et al*. schemes are presented in Table 1. Notice that the time complexities for performing the modular exponentiation, is $O(\log^3(N))$ [15]. Yet the time complexity for performing the one-way hash function depends on what cryptographic primitive it employed. It should be mentioned that in Table 1 the size of hash function is usually small and don't affect on communicational cost and also size of bit numbered N is bigger than other parameters. So in our proposed scheme value of $|N|$ is decreased.

In addition, the proposed scheme is improved in computational complexity because with considering computational complexity that we define, exponentiation calculating has most complexity and it could be decreased in the scheme.

Simulation Results: We also calculated the performance of our scheme by simulation to validate the results presented by Table 2. We simulated our protocol with the MATLAB framework. Signal range of mobile device is equal to 15 meters. Ten runs were conducted and each run corresponds to a particular deployment of 500 mobile devices. The network is assumed to be ideal i.e. there is no message loss, conflict in the network, etc. The node deployed in random positions. All the parameters of network are shown in Table 3. We used shortest path routing in the simulation in all of the methods. We used a radio setting model same as one in [16]. In this model we used Eq. 17 to transmit a message of length l between a cluster member and its cluster head and used Eq. 18 to transmit a message of length l between a cluster head and the base station. The following notations are used in performance evaluation:

$$E_{Tih} = lE_e + l\varepsilon_s d_{ih}^2 \quad (17)$$

$$E_{Thb} = lE_e + l\varepsilon_l d_{hb}^4 \quad (18)$$

$$E_R = lE_e + lE_{BF} \quad (19)$$

E_{Tih}: Energy of transmitting of length l bits between mobile device M and its cluster head h.

E_{Tih}: Energy of transmitting a message of length l bits between a cluster head h and the base station.

d_{ih}: Distance between mobile device M and its cluster head.

d_{hb}: Distance between cluster head h and the base station.

E_R: Energy of receiving a message of length l bits.

E_{BF}: Cost of beam forming approach to reduce energy consumption.

ε_S: Energy consumed by the amplifier to transmit at a short distance.

ε_L: Energy consumed by the amplifier to transmit at a long distance.

E_e: Energy consumed in the electronic circuit to transmit or receive the signal.

Values of these parameters are presented in Table 2.

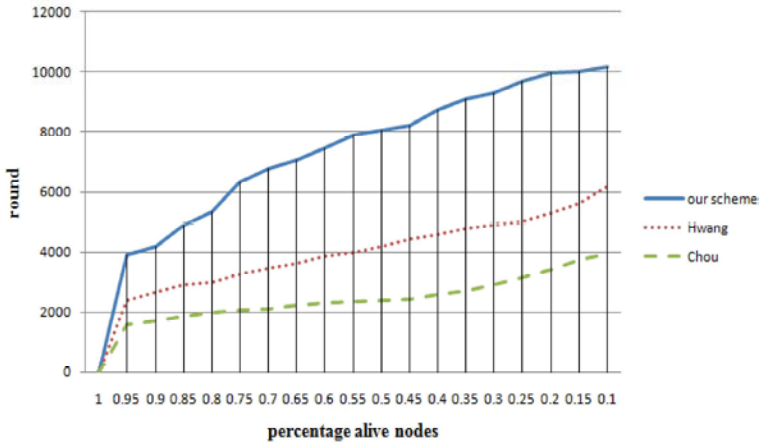

Fig. 3: Lifetime of the network for three schemes

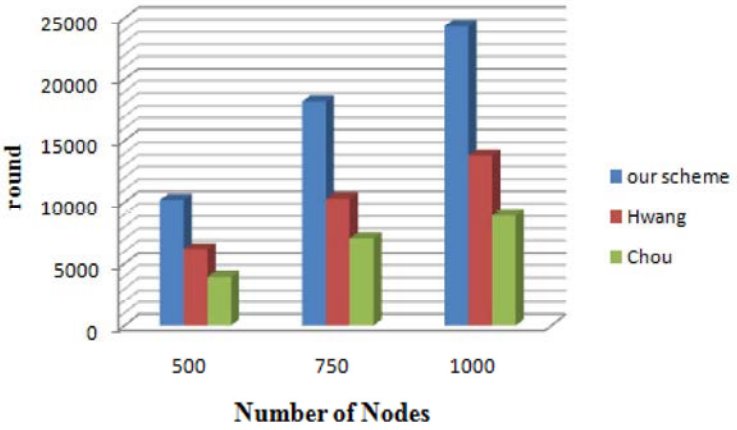

Fig. 4: Lifetime of the network for three schemes for different networks

Fig.3 shows the results of the simulation of the presented algorithm along with Hwang and Chou schemes. In this figure the lifetime of the network (based on the number of data gathering which we call round) for different algorithms is shown. Clearly, the lifetime of the network is significantly increased considerably using our scheme and the main reason in the length of transmitted packets.

We also carried out multiple experiments on networks of size ranging 500 to 1000 nodes. Fig. 4 shows the lifetimes of three discussed schemes in the networks with 500, 750 and 1000 nodes. You can notice that our proposed schemes prolong lifetime of networks.

CONCLUSION

In previously proposed schemes only mobile device can prove his authenticity to base station, but we proposed an efficient mutual identification scheme based on identity as mobile device and base station will confidence on each other's legitimacy. Also an efficient scheme is achieved that can be used in wireless environment at limited battery capacity. Simulation result show that proposed scheme is secure mutual identification scheme and can be used in wireless environment.

REFRENCES

1. Shamir, A., 1984. Identity Based Cryptosystem & Signature Scheme, *Advance in Cryptology CRYPTO'84*. Lecture Note-Computer Sci., pp: 47-53.
2. Tanaka, H., 1987. A Realization Scheme for the Identity-Based Cryptosystem, proc Crypto' pp: 340-349.
3. Tsai, Y.W. and T. Hwang, 1987. ID based pubic key cryptosystem based on Okamoto and Tanaka's ID based on one way communication scheme, Electronic Letters, 26(10): 666-668.

4. Tsujii, S., T. Itoh and K. Kurosawa, 1987. ID-based cryptosystem using discrete logarithm problem, Electron Letter, 23: 1318-1320.
5. Gunther, C.G., 1987. An identity-based key-exchange protocol, *Cryptology-Eurocrypt'86*. New York: Springer, pp: 29-37.
6. Okamato, E. and K. Tanaka, 1989. Identity-based information security management system for personal computer networks, IEEE J. Set Area Commun, 7(2): 290-294.
7. Lee, W.B. and K.C. Liao, 2004. Constructing identity based cryptosystems for discrete logarithm based cryptosystems, J. Network and Computer Applications, 27(4): 191-194.
8. Tseng, Y.M. and J.K. Jan, 1998. ID-based Cryptographic Scheme Using a Non-interactive Public-key Distribution System, Proceeding of the 14th Annual Computer Security Applications Conference, Phoenix, Arizona, pp: 237-243.
9. Hwang, M.S., J.W. Lo and S.C. Lin, 2004. An Efficient User Identification Scheme Based on ID-Based Cryptosystem, Computer Standard and Interfaces, 26(6): 565-569.
10. Chou, J.S., Y. Chen and C.H. Lin, 2006. An improvement of an efficient user identification scheme based on ID-based cryptosystem, Proc of the IEEE International Conference on Sensor Networks, 1(5): 558-561.
11. Chou, J.S., C.H. Lin and T.Y. Lee, 2004. A Novel Hierarchical Key Management Scheme Based on Quadratic Residues, ISPA2004, LNCS 3358, pp: 858-865.
12. Diffie, W. and M. Hellman, 1976. New Direction in Cryptography, IEEE Trans Inf Theory, 6: 644-654.
13. Kohl, J. and C. Neuman, 1993. The Kerberos Authentication Service (v5)," Internet REC, pp: 1510.
14. Maurer, U.M. and Y. Yacobi, 1996. A non-interactive public key distribution system, Designs, Codes and Cryptology, 9(3): 305-316.
15. Camenish, J., 1998. Group signature schemes and payment systems based on discrete logarithm problem, ETH series in information security and cryptography, vol.2, Konstanz: Hartuge-GorreVerlag; pp: 11-2.
16. Heinzelman, W.R., A. Chandrakasan and H. Balakrishnan, 2000. Energyefficient communication protocol for wireless microsensor networks, Proceedings of the Hawaii International Conference on System Sciences.