An Efficient and Robust User Authentication Scheme for Hierarchical Wireless Sensor Networks without Tamper-Proof Smart Card

Tanmoy Maitra[1], Ruhul Amin[2], Debasis Giri[3], and P. D. Srivastava[4]
(Corresponding author: Tanmoy Maitra)

Department of Computer Science & Engineering, Jadavpur University, Kolkata-700032, India[1]
Department of Computer Science & Engineering, Indian Schools of Mines University, Dhanbad-826004, Jharkhand, India[2]
Department of Computer Science & Engineering, Haldia Institute of Technology, Haldia-721657, India[3]
Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur-721302, India[4]
(Email: *tanmoy.maitra@live.com*) *(Received May 13, 2014; revised and accepted Aug. 20 & Nov. 3, 2014)*

Abstract

The cluster heads in hierarchical wireless sensor networks gather real time data from the other ordinary sensor nodes and send those data to a nearest base station. But, the main important issue is that how a user will get the real time data directly from a cluster head securely. To solve this problem, many user authentication schemes have been proposed in literature. In 2012, Das et al. proposed a dynamic password-based user authentication scheme for hierarchical wireless sensor networks and showed that their scheme is secure against all possible attacks. In this paper, we have pointed out that Das et al.'s scheme is insecure against insider attack, theft attack and session key recovery attack, and their scheme also suffers from dynamic cluster head addition overhead problem, limited number of cluster heads access problem and clock synchronization problem. To overcome these drawbacks, we have proposed an efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card in this paper. We have also shown that our scheme provides better tread-off among security and communication overhead compare to the Das et al.'s scheme.

Keywords: Authentication, Password, Smart Card, HWSN

1 Introduction

There are no proper ad hoc infrastructures in wireless sensor networks where a large number of sensor nodes are deployed by truck or plane on a target field. After deployment of sensor nodes, they communicate to other neighboring nodes within their communication range to form clusters. After that, one cluster head or gateway node is selected by base station or sensor nodes for each cluster on the basis of energy, signal strength, degree, capability, mobility etc. All the sensor nodes sense raw data from environment and send to their nearest cluster head by single-hop or multi-hop communication [21]. Cluster heads gather the raw data and send to nearest base station or sink node by multi-hop or single-hop communication [21]. Finally, data are collected from base station. The collected data is not always real time data because all cluster heads send data to base station after a certain periodic time. But, there is needed to collect real time data for taking immediate action in some application like Defense Advanced Research Project Agency (DARPA) [2]. If we collect data directly from cluster heads, we can get real time data. This is possible if it is allowed to access those real time data directly from cluster head, when demanded. Hence, it is needed to first authorize the accessors and then allows to access to do secure communication among accessors and cluster heads [7]. It should be noted that user authentication in wireless sensor networks satisfies all the following requirements:

1) Users can freely choose and update their passwords.
2) Low computational, storage and communication cost.
3) Session key agreements between cluster head and user.
4) Mutual authentication between users and base station and also between base station and cluster head.
5) Prevention of possible attacks.
6) Without maintaining password verification tables at server end.

The main goal in this paper is to design authentication scheme in such a manner that the designed protocol is better tread-off among security and communication cost than the previously published scheme. There exist many user authentication protocols in literature for wireless sensor network [3–5, 8, 9, 11, 14, 22–27].

In 2004, Watro et al. [25] proposed a user authentication scheme for wireless sensor networks, called Tinypk based on RSA [19] and Diffie-Hellman [6] protocols. In 2006, Wong et al. [26] described a user authentication scheme based on one way hash function and password. In 2007, Tseng et al. [22] proposed a dynamic user authentication scheme for wireless sensor networks. In 2009, Vaidya et al. [24] showed that Wong et al.'s scheme [26] suffers from forgery and replay attack, and Tseng et al.'s scheme [22] cannot thwart replay attack and man-in-the-middle (MITM) attack. Vaidya et al. [24] also proposed a robust dynamic user authentication scheme for wireless sensor networks. In the same year, M.L. Das [5] proposed an improved efficient scheme over Wong et al.'s scheme [26] based on user password and time stamp. But in 2010, Khan and Alghathbar [11] showed that M.L. Das's scheme [5] is insecure against gate-way node bypassing attack and privileged-insider attack. In 2010, He et al. [9] proposed an improved scheme over M.L. Das's scheme [5]. Later, Vaidya et al. [23] pointed out the insider attack and impersonation attack in both M.L. Das' scheme [5] and Khan and Alghathbar's scheme [11] and also proposed an improved two-factor user authentication scheme. In the same year, Fan et al. [8] proposed a user authentication scheme for two-tiered [13] wireless sensor networks. In 2010, Yuan et al. [27] pointed out that Watro et al.'s scheme [25] cannot resist forgery attack and proposed a biometric-based user authentication scheme for wireless sensor networks which is similar concept as in M.L. Das's scheme [5]. In 2011, Kumar and Lee [14] pointed out that He et al.'s scheme [9] is susceptible to information leakage attack and scheme [9] cannot preserve user anonymity, mutual authentication between a sensor and a user and does not establish the session key between the user and the sensor node. Kumar and Lee [14] also pointed out that Khan and Alghathbar's scheme [11] does not provide mutual authentication between the sensor and the user and does not establish the session key between the user and the sensor node with no confidentiality to their air messages.

In 2012, Das et al. [4] proposed a dynamic password-based user authentication scheme for hierarchical wireless sensor networks. In this paper, we have pointed out that their scheme is insecure against some attacks such as insider attack and session key recovery attack. Further, it is noted that base station uses user's secret parameter in the user's registration phase which is impossible. Additionally, their scheme suffers from dynamic cluster head addition overhead problem, limited number of cluster head access problem and clock synchronization problem. To overcome their weaknesses, we have proposed an efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card. Our scheme provides better security with low computational over head and low communication cost than Das et al.'s scheme [4].

The remainder of this paper is organized as follows: Section 2 shows network model concept. Section 3 shows brief review of Das et al.'s scheme. In Section 4, we show security weaknesses of Das et al.'s scheme. In Section 5, we propose our scheme. Section 6 shows security analysis of our proposed scheme. In Section 7, we compare the performances of our scheme with previously published scheme. Finally, we conclude the paper in Section 8.

2 Network Model

In hierarchical wireless sensor network (HWSN) (shown in Figure 1), there is a hierarchy among the nodes based on their capabilities namely, base station, cluster heads and sensor nodes. Usually, the ordinary sensor nodes are inexpensive, limited capabilities like, low battery power, low memory size, short transmission range, slow data processing etc. Cluster heads are little more expensive and has little more computational capability, battery power, memory size, transmission range than ordinary sensor nodes. However base station has unlimited battery power, huge memory size, extremely long transmission range with high computational capability and also an access point for human interface.

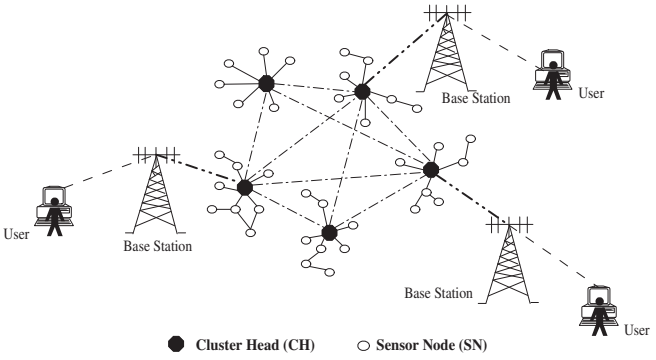

Figure 1: A hierarchical wireless sensor network (HWSN) architecture

In HWSN, all ordinary sensor nodes sense data from environment and send those sensed data to cluster head by single-hop or multi-hop communication [21]. Cluster head eliminates the redundancy data and aggregates all data and sends to base station via other cluster heads or directly. Then, a valid user can access those transmitted data from base station. Once the sensor nodes and cluster head are deployed, there is a problem for wireless sensor networks to maintain them. Limited battery power is responsible for limited life time of this networks. To maximize the life time of network it is necessary to design such a protocol that minimize the computational and communication cost of each node.

We consider the HWSN model for developing our proposed scheme due to the following reasons. Wireless sensor networks are distributed environment-driven systems that differ from traditional wireless networks in several ways, for examples, extremely high number of sensor nodes, data-centric network, broadcast communication paradigm and co-related data passing.

2.1 Assumptions

We have considered the following assumptions:

- There is a well established MAC protocol [18] to transmit data in networks.
- Base station can be considered as a trusted authority.
- The compromised (captured) nodes can be detected by base station and as a result, the base station, cluster head and sensor nodes know the identities of the compromised nodes. Consequently, the base station alerts the users with the compromised cluster heads.

3 Brief Review of Das et al.'s Scheme

In this section, we briefly describe Das et al.'s a dynamic password-based user authentication scheme for hierarchical wireless sensor networks [4]. The notations are used throughout this paper are summarized in Table 1.

Table 1: List of notation used

Symbol	Description
U_i	*i-th* User
BS	Base station
SN_j	Sensor node j
CH_j	Cluster head j in the *j-th* cluster
pw_i	Password of user U_i
ID_i	Identity of user U_i
ID_{CH_j}	Identity of cluster head CH_j
ID_{SN_j}	Identity of sensor node SN_j
S_{CH_j}	Shared secret key between CH_j and BS
S_{SN_j}	Shared secret key between SN_j and BS
MK_{CH_j}	Unique shared master key randomly generated by the BS for CH_j
SK	Shared session key between U_i and CH_j
$h(\cdot)$	Cryptographic One-way hash function
E	Symmetric key encryption algorithm
D	Symmetric key decryption algorithm
s	Secret information of the base station
X_A	Shared secret between U_i and BS
T	Current time stamp
$\|$	Concatenation operation
$\oplus$	Bit wise XOR operation

In Pre-deployment phase, base station assigns a unique identity, ID_{CH_j} and ID_{SN_j} for each cluster heads CH_j and each sensor node SN_j respectively. Base station also randomly selects unique master key MK_{CH_j} and MK_{SN_j} for each cluster heads CH_j and each sensor node SN_j respectively. These unique master keys MK_{CH_j} is shared between cluster head and base station, whereas MK_{SN_j} is shared between sensor node and base station. Then $\{ID_{CH_j}, MK_{CH_j}\}$ is stored into the memory of cluster head CH_j, and also $\{ID_{SN_j}, MK_{SN_j}\}$ is stored into the memory of sensor node SN_j. Finally these cluster heads and sensor nodes are dropped in a target field. Now for user authentication, their scheme consists of four phases namely, registration phase, login phase, authentication phase and password change phase.

3.1 Registration Phase

A user U_i selects a random number y_i, an identity ID_i and a password pw_i, and then computes $pwr_i = h(pw_i \| y_i)$. Then, U_i sends ID_i and pwr_i to the base station via a secure channel. After getting registration request message $\{ID_i, pwr_i\}$, base station computes $f_i = h(ID_i \| s)$, $x = h(pwr_i \| X_A)$, $r_i = h(y_i \| x)$, $e_i = f_i \oplus x$. Base station then selects $m + m'$ number of deployed cluster heads with $m + m'$ number of key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 < j \leq m + m'\}$, where $K_j = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| s)$. Finally, base station stores $\langle ID_i, y_i, X_A, r_i, e_i, h(\cdot)$ and $m + m'$ key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 < j \leq m + m'\}\rangle$ into the memory of a tamper-proof smart card of user U_i and issues that smart card for user U_i.

3.2 Login Phase

User U_i inserts his/her smart card to the card reader and then provides ID_i and pw_i. The card reader computes $pwr'_i = h(y_i \| pw_i)$, $x' = h(pwr'_i \| X_A)$, $r'_i = h(y_i \| x')$ and checks whether computed r'_i equals stored r_i or not. If equal, card reader further computes $N_i = h(x' \| T_1)$, where T_1 is the current time stamp of user U_i and a ciphertext $E_{K_j}(ID_i \| ID_{CHj} \| N_i \| e_i \| T_1)$, where ID_{CHj} is chosen by the user U_i. Finally, U_i sends the login request message $msg = \{ID_i \| ID_{CH_j} \| E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1)\}$ to the base station over a public channel.

3.3 Authentication Phase

After receiving the login request message $msg = \{ID_i \| ID_{CH_j} \| E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1)\}$ from the user U_i, the base station computes key $K = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| s)$ and by the computed key K, base station decrypts ciphertext $E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1)$ and thus, $D_K(E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1))$ and verifies the validity of ID_i, ID_{CH_j} and T_1. If all are correct then base station further computes $X = h(ID_i \| s)$, $Y = e_i \oplus X$ and $Z = h(Y \| T_1)$ and verifies

whether $Z = N_i$ or not. If it holds then base station computes $u = h(Y \parallel T_2)$, where T_2 is the current time stamp of base station and produces a ciphertext message encrypted using the master key MK_{CH_j} of the cluster head CH_j as $E_{MK_{CH_j}}(ID_i \parallel ID_{CH_j} \parallel u \parallel T_1 \parallel T_2 \parallel X \parallel e_i)$ and sends the message $\{ID_i \parallel ID_{CH_j} \parallel E_{MK_{CH_j}}(ID_i \parallel ID_{CH_j} \parallel u \parallel T_1 \parallel T_2 \parallel X \parallel e_i)\}$ to the corresponding cluster head CH_j. After receiving message from base station, CH_j decrypts this message by computing $D_{MK_{CH_j}}(E_{MK_{CH_j}}(ID_i \parallel ID_{CH_j} \parallel u \parallel T_1 \parallel T_2 \parallel X \parallel e_i))$ and checks the validity of ID_i, ID_{CH_j} and T_2. If all are valid then, CH_j further computes $v = e_i \oplus X$ and $w = h(v \parallel T_2)$ and checks whether $w = u$ or not. If it is true, then the user U_i is considered as a valid user and authenticated by CH_j and computes a session key $SK = h(ID_i \parallel ID_{CH_j} \parallel e_i \parallel T_1)$. Finally, CH_j sends an acknowledgment to the user U_i via other cluster heads and the base station, and responds to the query of the user U_i. After receiving the acknowledgment from CH_j, the user U_i agrees with the same secret session key SK, shared with CH_j by computing $SK = h(ID_i \parallel ID_{CH_j} \parallel e_i \parallel T_1)$ and they will use SK for securing communications in future.

3.4 Password Change Phase

This phase is invoked when user U_i wants to change his/her password. U_i inserts the smart card to the card reader and submits ID_i and pw_i. The card reader computes $pwr'_i = h(y_i \parallel pw_i)$, $x' = h(pwr'_i \parallel X_A)$, $r'_i = h(y_i \parallel x')$ and checks whether computed r'_i equals stored r_i or not. If equal, U_i enters a new password pw_i^{new}. Then the card reader further computes $M_1 = e_i \oplus x'$, $M_2 = h(y_i \parallel pw_i^{new})$, $r_i^{new} = h(y_i \parallel M_2)$, $M_3 = h(M_2 \parallel X_A)$, $e_i^{new} = M_1 \oplus M_3$. Finally, replace r_i with r_i^{new} and e_i with e_i^{new} into the memory of the smart card.

4 Weaknesses of Das et al.'s Scheme

In this section, we first describe the security weaknesses and then discuss the advantages of Das et al.'s scheme [4].

4.1 Security Weaknesses

In this section, we will analyze the security of Das et al.'s scheme [4]. In 2013, Li et al. [15] showed that Das et al.'s scheme [4] is insecure against off-line password guessing attack, impersonation attack, compromised cluster head attack and many logged-in users' attack. Except these attacks, Das et at.'s scheme [4] is insecure against insider attack, session key recovery attack and theft attack. To analyze the above weaknesses, we will assume that an attacker can obtain the secret parameter stored in the smart card by monitoring power consumption [12, 16] and can intercept all communicating message among user, base station and cluster head.

4.1.1 Insider Attack

A random number y_i is chosen by user U_i and y_i is not send by the user U_i to base station in registration phase of Das et al.'s scheme [4]. But in their scheme, base station uses y_i to compute $r_i = h(y_i \parallel x)$ which is impractical. Now, if we assume that user U_i also sends y_i to the base station, insider attack will be mounted against in their scheme because system manager or privileged insider of the base station knows pwr_i, y_i and $h(\cdot)$. So, easily system manager or privileged insider of the base station can guess the user's correct password by performing the following:

Computes $pwr_i^* = h(y_i \parallel pw_i^*)$ after choosing a guessed password pw_i^* and then, checks pwr_i^* and pwr_i are equal or not. If not equal, chooses another pw_i^* and repeats $pwr_i^* = h(y_i \parallel pw_i^*)$ until correct password is obtained. Otherwise pw_i^* is the correct password of the user U_i. That is after some guessing, system manager or privileged insider of the base station can find out the correct password of the user U_i as it is low entropy.

4.1.2 Theft Attack

We assume that an attacker knows valid password pw_i of a user U_i as shown in [15] and stored secret parameters of the smart card by monitoring power consumption [12,16]. To get success on the theft attack, an attacker have to steal user's smart card and computes the following steps:

Step 1. Attacker can compute $h(ID_i \parallel s)$ by computing $h(ID_i \parallel s) = e_i \oplus h(h(y_i \parallel pw_i) \parallel X_A)$, where attacker knows correct password pw_i and stored smart card's parameters X_A, e_i and y_i.

Step 2. Then, attacker chooses new password $pw_i^\dagger$ and random number $y_i^\dagger$ and, computes $pwr_i^\dagger = h(y_i^\dagger \parallel pw_i^\dagger)$, $x^\dagger = h(pwr_i^\dagger \parallel X_A)$, $r_i^\dagger = h(y_i^\dagger \parallel x^\dagger)$ and $e_i^\dagger = h(ID_i \parallel s) \oplus x^\dagger$.

Step 3. Finally, attacker loads $r_i^\dagger$, $y_i^\dagger$ and $e_i^\dagger$ into the memory of his/her smart card and keeps all other parameters $\langle ID_i, X_A, h(\cdot)$ and $m + m'$ key-plus-id combinations $(K_j, ID_{CH_j})\rangle$ unchanged. Then, uses his/her smart card as it is used by U_i.

4.1.3 Session Key Recovery Attack

We assume that an attacker can extract the secret information by monitoring power consumption [12, 16] from user U_i's smart card and also can intercept the all $i-th$ communicating messages among user U_i, base station BS and cluster head CH_j. After getting (K_j, ID_{CH_j}) combinations by monitoring the power consumption, an attacker can perform the session key recovery attack successfully as follows:

Step 1. An attacker intercepts the user U_i's login message $\{ID_i \parallel ID_{CH_j} \parallel E_{K_j}(ID_i \parallel ID_{CH_j} \parallel N_i \parallel e_i \parallel T_1)\}$.

Step 2. Attacker decrypts ciphertext $E_{K_j}(ID_i \parallel ID_{CH_j} \parallel N_i \parallel e_i \parallel T_1)$ by using K_j to get e_i and T_1, where K_j is stored into the memory of smart card of U_i.

Step 3. Attacker computes session key SK^* between user U_i and cluster head CH_j by performing $h(ID_i \parallel ID_{CH_j} \parallel e_i \parallel T_1)$ which is equal to session key between user U_i and cluster head CH_j.

Hence, the above procedure shows that Das et al.'s scheme [4] is insecure against the session key recovery attack.

4.2 Disadvantages of Das et al.'s Scheme

In this subsection, we will point out some disadvantages of Das et al.'s scheme [4].

4.2.1 Dynamic Cluster Head Addition Over Head Problem

In dynamic node addition phase of scheme [4], it is mentioned that no other information regarding cluster heads addition is required to store in the user's smart card. But, whenever new cluster heads are deployed, base station has to store their key-plus-id combinations $(K_{m+j}, ID_{CH_{m+j}})$ into the memory of user U_i's smart card, because user U_i cannot compute $\{K_{m+j} = E_{MK_{CH_{m+j}}}(ID_i \parallel ID_{CHm+j} \parallel s) \mid (m+j) > (m+m')\}$ without knowing the secret key s of base station and shared secret key $MK_{CH_{m+j}}$ between newly added cluster head CH_{m+j} and base station. Hence, dynamic cluster head addition increases the computation overhead of base station for storing key-plus-id combinations for each users.

4.2.2 Limited Number of Cluster Head Access Problem

Das et al. [4] mentioned that $(m+m')$ is chosen according to the memory availability of the smart card. Let, memory availability of the smart card is for 200 cluster heads' key-plus-id combinations. Thus, we can store key-plus-id combinations of 200 cluster heads into the memory of the smart card. It can be assumed that already 200 cluster heads are present into the network. Later, if we deploy more sensor nodes (including cluster heads) in the network for some reason then users cannot get real-time data from the newly deployed cluster heads because there are no memory space to store key-plus-id combinations of newly deployed cluster heads into the memory of smart card. Hence, the main objective of this architecture will be hampered.

4.2.3 Time Synchronization Problem

As Das et al. [4] used time stamp in their scheme, there is a probability of time synchronization problem between base station and user. Also same problem can be occurred between cluster head and base station during communication.

5 Our Proposed Scheme

In this section, we will propose an efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card. Our scheme consist of seven phases, namely pre-deployment phase, post-deployment phase, user registration phase, user login phase, authentication phase, password change phase and dynamic node addition phase.

5.1 Pre-deployment Phase

Base station performs following steps before deployment of cluster heads and ordinary sensor nodes on a target field. Figure 2 shows the pre-deployment phase of our proposed scheme.

Step 1. Base station chooses a random number c_j and an identity ID_{CH_j}, $(1 \leq j \leq m)$ for each cluster head CH_j. Then, it computes $S_{CH_j} = h(s \parallel ID_{CH_j} \parallel c_j)$ and stores $\{ID_{CH_j}, S_{CH_j}\}$ into the memory of CH_j as tamper resists.

Step 2. It chooses a random number w_p and an identity ID_{SN_p}, $(1 \leq p \leq x)$ for each ordinary sensor node SN_p. Then, it computes $S_{SN_p} = h(s \parallel ID_{SN_p} \parallel w_p)$ and stores $\{ID_{SN_p}, S_{SN_p}\}$ into the memory of SN_p as tamper resists.

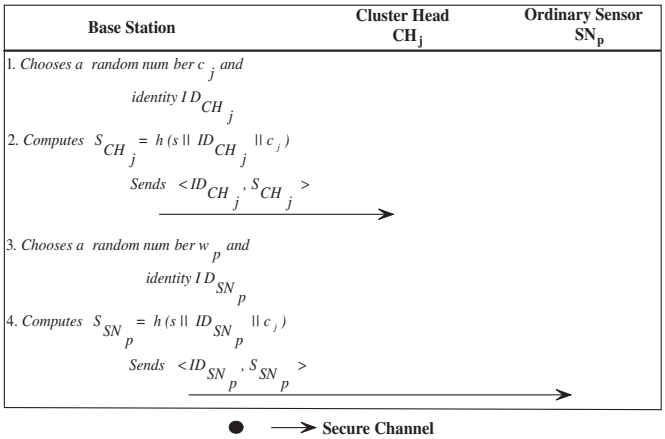

Figure 2: Pre-deployment phase

5.2 Post-deployment Phase

After deployment of cluster heads and ordinary sensor nodes on a target field, they form clusters such a way [10] that for each cluster, there will be a cluster head. The main objective in this paper is that how a valid user U_i, where $(1 \leq i \leq z)$ securely communicates to a cluster head CH_j to get real time data from target field.

5.3 User Registration Phase

In this phase, a user U_i chooses a random number y_i, his/her identity ID_i and password pw_i. Then, U_i computes $pwr_i = h(pw_i \parallel y_i)$ and sends $\{ID_i, pwr_i\}$ to the base station BS through a secure channel. After getting message $\{ID_i, pwr_i\}$ from the user U_i, base station computes $X_i = h(ID_i \parallel s) \oplus pwr_i$ and $B_i = h(h(ID_i \parallel s) \parallel pwr_i)$. Then base station issues a smart card for user U_i by storing $\{X_i, B_i, h(\cdot)\}$ into the memory of smart card. After getting his/her smart card, user U_i stores y_i into the memory of smart card. Figure 3 shows the user registration phase of our proposed scheme.

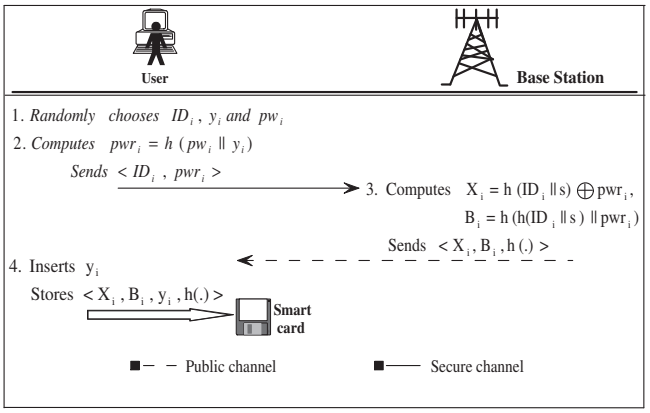

Figure 3: User registration phase

5.4 User Login Phase

In this phase, user U_i provides his/her identity ID_i and password pw_i to the card reader. Then card reader computes $pwr'_i = h(pw_i \parallel y_i)$, $Y'_i = X_i \oplus pwr'_i$, $B'_i = h(Y'_i \parallel pwr'_i)$ and checks whether computed B'_i equals stored B_i. If true, proceed to next otherwise 'rejects' user U_i. Then, user U_i chooses ID_{CH_j} and submits it to the card reader. Then, card reader further chooses a random number N_1 and computes $P_i = h(Y'_i \parallel ID_{CH_j} \parallel N_1 \parallel pwr'_i)$ and $R_i = N_1 \oplus pwr'_i$ and sends $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ to the base station. Figure 4 shows the user login phase of our proposed scheme.

5.5 Authentication Phase

In this phase, after getting login request message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ from user U_i, base station computes $Y_i^* = h(ID_i \parallel s)$, $pwr_i^* = Y_i^* \oplus X_i$, $N_1^* = pwr_i^* \oplus R_i$ and $P_i^* = h(Y_i^* \parallel ID_{CH_j} \parallel N_1^* \parallel pwr_i^*)$ and, it checks whether computed P_i^* equals sending P_i or not. If it holds good, base station further chooses a random number N_2 and computes $Z_i = pwr_i^* \oplus N_2$, $D_i = h(Y_i^* \parallel N_2 \parallel ID_{CH_j} \parallel ID_i \parallel N_1^*)$. Then, it sends $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ to the user U_i. Again base station computes $N_3 = N_2 \oplus N_1^*$, $V_i = h(ID_{CH_j} \parallel S_{CH_j})$, $E_i = V_i \oplus N_3$, $A_i = h(Y_i^* \parallel N_3 \parallel pwr_i^*)$, $L_i = A_i \oplus V_i$ and

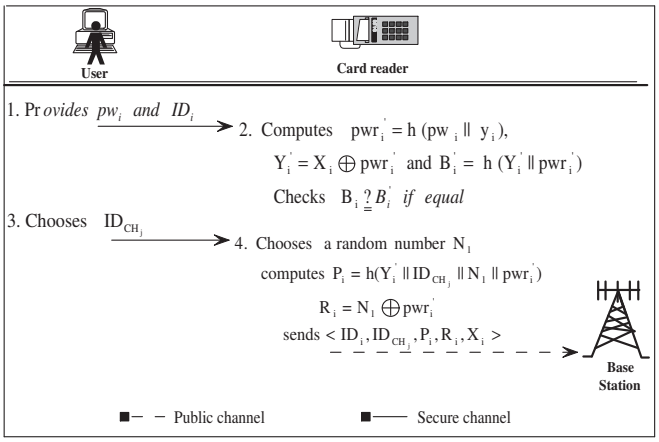

Figure 4: User login phase

$G_i = h(S_{CH_j} \parallel N_3 \parallel A_i \parallel ID_i \parallel ID_{CH_j})$ and, sends $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ to the cluster head CH_j. After that the following computations are performed:

1) After getting reply message $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ from base station, card reader computes $N'_2 = Z_i \oplus pwr'_i$, $D'_i = h(Y'_i \parallel N'_2 \parallel ID_{CH_j} \parallel ID_i \parallel N_1)$ and checks whether computed D'_i equals sending D_i or not. If it holds good then computes $N'_3 = N_1 \oplus N'_2$, $A'_i = h(Y'_i \parallel N'_3 \parallel pwr'_i)$ and session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N'_3 \parallel A'_i)$.

2) After receiving message $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ from base station, cluster head CH_j computes $V_i^\star = h(ID_{CH_j} \parallel S_{CH_j})$, $N_3^\star = V_i^\star \oplus E_i$, $A_i^\star = L_i \oplus V_i^\star$ and $G_i^\star = h(S_{CH_j} \parallel N_3^\star \parallel A_i^\star \parallel ID_i \parallel ID_{CH_j})$ and checks weather computed $G_i^\star$ equals sending G_i or not. If true, then it computes session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N_3^\star \parallel A_i^\star)$.

Now, both parties (user U_i and cluster head CH_j) are agreed with common shared session key SK and can communicate securely to each other by shared secret session key SK in future. Figure 5 shows the authentication phase of our proposed scheme.

5.6 Password Change Phase

In this phase, user U_i provides his/her identity ID_i and password pw_i to the card reader. Card reader computes $pwr'_i = h(pw_i \parallel y_i)$, $Y'_i = X_i \oplus pwr'_i$, $B'_i = h(Y'_i \parallel pwr'_i)$ and checks whether B'_i equals B_i or not. If equal, proceed to next otherwise 'rejects' user U_i. Then, user U_i provides new password pw_i^{new} to the card reader. Card reader computes $pwr_i^{new} = h(pw_i^{new} \parallel y_i)$, $X_i^{new} = Y'_i \oplus pwr_i^{new}$, $B_i^{new} = h(Y'_i \parallel pwr_i^{new})$. Then U_i replace old values of X_i and B_i by the new value of X_i^{new} and B_i^{new} respectively into the memory of smart card. Thus, U_i can change the password without taking any assistance from base station.

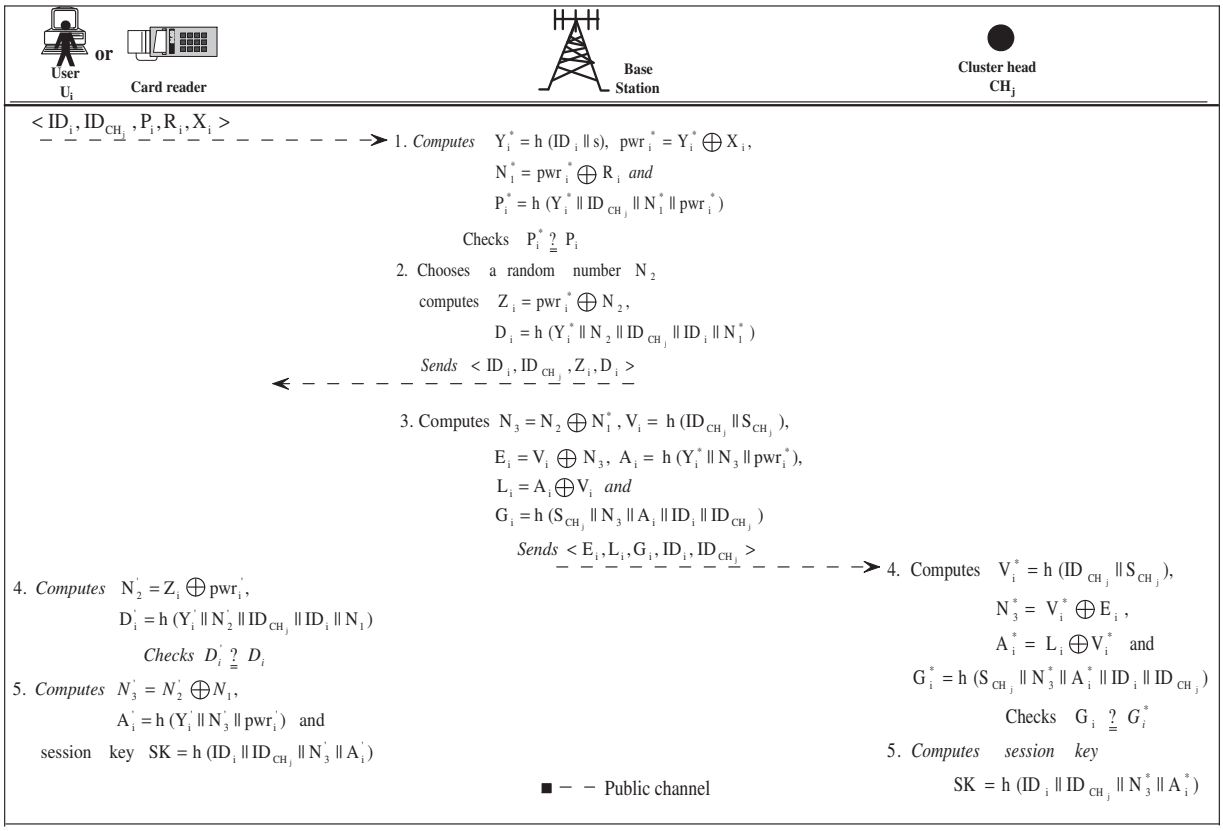

Figure 5: Authentication phase

5.7 Dynamic Node Addition Phase

In this phase, we describe the addition or replace procedure of new nodes into the networks of our scheme. This phase is needed to replace or add new nodes which are either dead for energy loss or captured by an attacker. Base station performs following steps:

Step 1. It chooses a random number c_l and an identity ID_{CH_l}, $(1 \leq l \leq m_1)$ for each cluster head CH_l. Then computes $S_{CH_l} = h(s \parallel ID_{CH_l} \parallel c_l)$ and stores $\{ID_{CH_l}, S_{CH_l}\}$ into the memory of CH_l as tamper resists.

Step 2. It chooses a random number w_v and an identity ID_{SN_v}, $(1 \leq v \leq x_1)$ for each ordinary sensor node SN_v. Then it computes $S_{SN_v} = h(s \parallel ID_{SN_v} \parallel w_v)$ and stores $\{ID_{SN_v}, S_{SN_v}\}$ into the memory of SN_v as tamper resists.

Step 3. All new nodes are deployed into the target field and then base station informs to the users about the addition of new nodes.

The above procedure shows that it is not needed to store information regarding new nodes into the memory of user's smart card.

6 Security Analysis of Our Proposed Scheme

In this section, we will analyze the security of our proposed scheme. We may assume that an attacker could obtain the values which are stored in the memory of smart card by monitoring the power consumption [12,16]. Further, attacker can intercept communicating messages among user, server and cluster head. Under these assumptions, we will show that the proposed scheme resists different possible attacks.

6.1 Smart Card Stolen Attack

We assume that user U_i has either lost his/her smart card or stolen by an attacker. After getting the smart card, an attacker can extract the parameters X_i, B_i, y_i and $h(\cdot)$ from the smart card of the user U_i. After getting all these parameters, it is hard to derive or guess user's correct password pw_i and base station's secret key s by the attacker as shown in following.

1) From parameter $X_i = h(ID_i \parallel s) \oplus pwr_i = h(ID_i \parallel s) \oplus h(pw_i \parallel y_i)$, given ID_i and y_i, attacker cannot guess s and pw_i because it is hard to guess two unknown parameters in polynomial time as shown by Sood et al. [20].

2) The attacker cannot compute s and pw_i from parameter $B_i = h(h(ID_i \parallel s) \parallel pwr_i) = h(h(ID_i \parallel s) \parallel h(pw_i \parallel y_i))$, given ID_i and y_i because it is computationally hard due to inverse of cryptographic one-way hash function.

So, the attacker cannot compute any secret information from parameters which are stored into the memory of smart card. Hence, the proposed scheme resists smart card stolen attack.

6.2 Impersonation Attack

To impersonate as a legitimate user, an attacker attempts to make a forged login request message $\{ID_i, ID_{CH_j}, P_i^a, R_i^a, X_i\}$ by computing following steps, given $\{X_i, B_i, y_i, h(\cdot), ID_i, ID_{CH_j}\}$

1) The attacker chooses random number N_1^a and also chooses a password pw_i^a.

2) Computes $pwr_i^a = h(pw_i^a \parallel y_i)$.

3) Computes $R_i^a = N_1^a \oplus pwr_i^a$.

But, to compute parameter $P_i^a = h(Y_i' \parallel ID_{CH_j} \parallel N_1^a \parallel pwr_i^a)$, where $Y_i' = h(ID_i \parallel s)$, attacker have to know secret key s of base station. In our scheme, secret key s of base station is used as $h(ID_i \parallel s)$. So, attacker cannot compute s from $h(ID_i \parallel s)$ because it is hard due to inversion of cryptographic one-way hash function. Thus, the attacker cannot produce forged login request message $\{ID_i, ID_{CH_j}, P_i^a, R_i^a, X_i\}$ in our scheme.

6.3 Privileged Insider Attack

If the system manager or privileged insider of the base station knows user's password, he/she may try to access user U_i's other accounts of other base stations. But in our scheme, $pwr_i = h(pw_i \parallel y_i)$, where random number y_i is unknown to the system manager or privileged insider of the base station is transmitted instead of pw_i to the base station in registration phase. From parameter pwr_i, privileged insider of the base station cannot compute correct pw_i because it is computationally hard due to inversion of cryptographic one-way hash function. So, the proposed scheme resists privileged insider attack.

6.4 Replay Attack

An attacker intercepts a valid login message $\{ID_i, ID_{CHj}, P_i, R_i, X_i\}$ and stores it for further use. After completion of user's transaction, base station stores this login message. Suppose, then the attacker sends the same stored login message to the base station. After receiving it, base station will check sending login message with stored login message and if both are equal then base station will reject the attacker's login request. In our scheme, $P_i = h(Y_i' \parallel ID_{CH_j} \parallel N_1 \parallel pwr_i')$ and $R_i = N_1 \oplus pwr_i'$. Our scheme resists replay attack because login message is changed in every session due to random number N_1.

6.5 Off-line Password Guessing Attack

We have shown in smart card stolen attack (Subsection 6.1) of our scheme that adversary cannot extract user U_i's password pw_i from smart card's parameters $\{X_i, B_i, y_i\}$. Again, the adversary try to guess user U_i's password pw_i from login message $\{ID_i, ID_{CHj}, P_i, R_i, X_i\}$ between user U_i and base station. But, we will show that the adversary cannot guess user U_i's password pw_i from login message which is as follows:

1) From parameter $P_i = h(Y_i' \parallel ID_{CH_j} \parallel N_1 \parallel pwr_i') = h(Y_i' \parallel ID_{CH_j} \parallel N_1 \parallel h(pw_i \parallel y_i))$, given ID_i, ID_{CHj} and y_i, adversary cannot guess password pw_i because it is hard due to inversion of cryptographic one-way hash function.

2) From parameter $R_i = N_1 \oplus pwr_i' = N_1 \oplus h(pw_i \parallel y_i)$, given y_i, adversary cannot guess user U_i's password because he/she have to solve parameter R_i without knowing two unknown values pw_i and N_1 which is computationally hard.

The above explanation shows that our proposed scheme resists off-line password guessing attack.

6.6 Theft Attack

If an adversary can store valid smart card's parameters into the memory of his/her smart card then the authentication scheme will be insecure against theft attack. In our scheme, to compute smart card's parameters, an adversary have to know valid user's password pw_i and secret key s of the base station. But, we have shown in smart card stolen attack (Subsection 6.1) that an adversary cannot compute base station's secret key and user's password from valid user's smart card. As a result, the proposed scheme is secure against theft attack.

6.7 Session Key Recovery Attack

In our scheme, an attacker cannot compute secret session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N_3 \parallel A_i) = h(ID_i \parallel ID_{CH_j} \parallel N_3 \parallel h(Y_i \parallel N_3 \parallel pwr_i)) = h(ID_i \parallel ID_{CH_j} \parallel N_3 \parallel h(h(ID_i \parallel s) \parallel N_3 \parallel h(pw_i \parallel y_i)))$ between user U_i and cluster head CH_j except captured cluster heads because, in our scheme, computation of session key depends on user's password pw_i, random number N_3 and secret key s of base station. We have shown in smart card stolen attack (Subsection 6.1) and off-line password guessing attack (Subsection 6.5) that the adversary has no way to get secret key s of base station and user's password pw_i. So, our scheme is secure against session key recovery attack.

Table 2: Comparison of computational cost of our scheme with Das et al.'s scheme

Schemes	Registration Phase		Login Phase	Authentication Phase		
	User	Base station	User	Base station	Cluster head	User
Das et al. [4]	$1T_h$	$(m+m')T_{enc}+3T_h$	$4T_h+1T_{enc}$	$3T_h+2T_{enc}+1T_{dec}$	$2T_h+1T_{dec}$	$1T_h$
Our	$1T_h$	$2T_h$	$3T_h$	$6T_h$	$3T_h$	$3T_h$

6.8 Denial of Service Attack

In password change phase of our proposed scheme, card reader first checks the validity of provided old password of any user say, U_i. If provided password is valid then only card reader allows user U_i to provide his/her new password. So, an adversary have to know the correct password of user U_i to change U_i's password. But, off-line password guessing attack (Subsection 6.5) shows that there is no chance to compute U_i's password. So, adversary cannot change password of user U_i. Thus, only valid users get service from cluster heads via base station. So, our scheme is secure against denial of service (DoS) attack.

6.9 Cluster Head Capture Attack

When a cluster head is compromised by an attacker then it compromises its own secret key and shared session key. Moreover, secure communication with users and with its neighbor sensor nodes are compromised. But in our scheme, there are a unique secret key is given for each node (including cluster head). Thus, if an attacker captures a cluster head, he/she will get secret key of that captured cluster head only. As a result, all other non-compromised cluster heads can still communicate securely with other nodes in the networks and with users. Hence, our scheme provides security against cluster head capture attack.

7 Performance Analysis of Our Proposed Scheme

In this section, we compare the performance of our proposed scheme with Das et al.'s scheme [4]. We assume that Das et al.'s scheme consist of $m+m^{'}=200$ nodes in the wireless sensor network. Table 2 shows the computation over head of user, base station and cluster head of our proposed scheme with the related scheme. Table 3 shows the communication cost and storage cost of our scheme and related scheme. In Table 2, T_h is the time required for hashing operation, T_{enc} is the time required for encryption operation and T_{dec} is the time required for decryption operation. In scheme [4], computational over head is directly proportional to number of cluster heads. But in our scheme, computation over head is independent on the number of cluster heads. Our proposed scheme takes less computational cost than that of Das et al.'s scheme.

For comparison purpose, we assume that the length of ID_i, ID_{CH_j}, X_A are 64 bits each, random nonce and message digest $h(\cdot)$ are 128 bits each. We may assume that AES-128 symmetric key encryption/decryption algorithm [17] are used in scheme [4]. In Table 3, we have shown the communication cost (capacity of transmitting message) of our scheme and scheme [4] is 1408 bits and 1536 bits respectively. So our scheme takes $(1536-1408) = 128$ bits less than that of the scheme of Das et al. [4]. Also the storage cost (stored in the memory of smart card) of our scheme and Das et al.'s scheme [4] are 512 bits and 32640 bits respectively. So, Das et al.'s scheme [4] takes $(32640-512) = 32128$ bits more than that of our scheme. Note that, storage cost dependent on the number of cluster heads in Das et al.'s scheme.

Table 3: Comparison of communication cost, storage cost and security attacks of our scheme with Das et al.'s scheme

Cost & Attack	Das et al. [4]	Our
Communication Cost	1536 bits	1408 bits
Storage Cost	32640 bits	512 bits
A1	√	×
A2	√	×
A3	√	×
A4	×	×
A5	√	×
A6	√	×
A7	√	×

A1: Insider Attack, A2: Off-line Password Guessing Attack, A3: Smart Card Stolen Attack, A4: Replay Attack, A5: Theft Attack, A6: Password Change Attack and A7: Session Key Recovery Attack

Most wireless sensor networks suffers from power consumption of cluster head. So low computation cost of cluster head is desirable. In Table 2, we have shown that the computation overhead of cluster head of our scheme with Das et al.'s scheme [4]. Das et al.'s scheme [4] takes more computation cost than that of our scheme.

In Table 3, we have shown that our scheme provide strong authentication system compared to Das et al.'s scheme [4]. Hence, our scheme provides batter security, low computational cost, low communication cost and storage cost than Das et al.'s scheme [4].

We will discuss the advantages of our proposed scheme over Das et al.'s scheme [4].

Mutual Authentication. Our scheme provides strong mutual authentication between a user and base station. Even if attacker can extract the secret information from the memory of user's smart card and intercepting login message between the user and base station, attacker cannot compute the valid login message and reply message without knowing the secret password pw_i of user U_i, secret key s of base station and random number N_1. So our scheme provides mutual authentication between a user and base station.

Early Wrong Password Detection. If the user U_i inputs a wrong password by mistake in password change phase or login phase, it will be quickly detected by the card reader itself since card reader computes $pwr'_i = h(pw_i \parallel y_i)$, $Y'_i = X_i \oplus pwr'_i$, $B'_i = h(Y'_i \parallel pwr'_i)$ and checks whether computed B'_i equals stored B_i into memory of smart card. Hence our scheme provides early wrong password detection.

Solves Time Synchronization Problem. Our proposed scheme uses randomly generated nonce N_1 and N_2 instead of time stamps to avoid time synchronization problem.

Unlimited Number of Cluster Head Access. In our scheme, we do not need to store any key-plus-id combinations for each cluster heads into the memory of user's smart card. In our scheme, stored parameters of user's smart card are independent of cluster head's secret information. Thus in our scheme, a user can access all the cluster heads (including newly deployed cluster heads) in the networks.

No Dynamic Cluster Head Addition Over Head. In our scheme, smart card's stored information are independent from any cluster head's information. Thus for addition of new nodes, base station does not need to compute further information regarding newly deployed cluster heads for user's smart card.

8 Conclusion

We have shown that Das et al.'s scheme suffers from some security weaknesses. To over come these weaknesses, we have proposed our scheme. Further, in security analysis, we have shown that our scheme is more efficient in terms of computational, communication and storage cost than that of Das et al.'s scheme. We have also shown that in our scheme, users can access all the cluster heads and no need to compute any parameter for the user's smart card after adding new cluster heads into the network. In future, validation of the proposed scheme will be evaluated by Automated Validation of Internet Security Protocols and Applications (AVISPA) [1], a security tool. Further, it can be incorporated biometric features into the proposed scheme to achieve high security in remote user authentication scheme.

References

[1] AVISPA, *Automated Validation of Internet Security Protocols and Applications*, Project funded by the European Community under the Information Society Technologies Programme, IST-2001-39252, 2001. (`http://www.avispa-project.org/`)

[2] DARPA, *Defense Advanced Research Projects Agency*, Section 2352, Title 10 of the United States Code, 2015. (`http://www.darpa.mil/our-research`)

[3] A. K. Das, "Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks," *International Journal of Network Security*, vol. 14, no. 1, pp. 1–21, 2012.

[4] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646–1656, 2012.

[5] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[7] F. Dressler, "Authenticated reliable and semi-reliable communication in wireless sensor networks," *International Journal of Network Security*, vol. 7, no. 1, pp. 61–68, 2008.

[8] R. Fan, L. di Ping, J. Q. Fu, and X. Z. Pan, "A secure and efficient user authentication protocol for two-tiered wireless sensor networks," in *Second Pacific-Asia Conference on Circuits, Communications and System (PACCS'10)*, vol. 1, pp. 425–428, 2010.

[9] D. He, Yi Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc & Sensor Wireless Networks*, vol. 10, no. 4, pp. 361–371, 2010.

[10] L. Jia, R. Rajaraman, and T. Suel, "An efficient distributed algorithm for constructing small dominating sets," *Distributed Computing*, vol. 15, no. 4, pp. 193–205, 2002.

[11] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[12] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'99)*, pp. 388–397, 1999.

[13] V. A. Kottapalli, A. S. Kiremidjian, J. P. Lynch, E. D. Carryer, T. W. Kenny, K. H. Law, and Y. Lei, "Two-tiered wireless sensor network architecture for structural health monitoring," in *Smart Structures and Materials*, pp. 8–19, 2003.

[14] P. Kumar and H. J. Lee, "Cryptanalysis on two user authentication protocols using smart card for

wireless sensor networks," in *Wireless Advanced (WiAd'11)*, pp. 241–245, 2011.

[15] C. Ta Li, C. Y. Weng, C. C. Lee, C. W. Lee, P. N. Chiu, and C. Yi Wu, "Security flaws of a password authentication scheme for hierarchical wsns," *Journal of Advances in Computer Network*, vol. 1, no. 2, pp. 121–124, 2013.

[16] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[17] NIST, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, National Institute of Standards and Technology (NIST), U. S. Department of Commerce, 2001. (`http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`)

[18] S. Ray, I. Demirkol, and W. Heinzelman, "ATMA: Advertisement-based tdma protocol for bursty traffic in wireless sensor networks," in *IEEE Global Telecommunications Conference (GLOBECOM'10)*, pp. 1–5, 2010.

[19] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communnications of ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[20] 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, no. 2, pp. 609–618, 2011.

[21] M. T. Thai, F. Wang, D. Liu, S. Zhu, and D. Z. Du, "Connected dominating sets in wireless networks with different transmission ranges," *IEEE Transactions on Mobile Computing*, vol. 6, no. 7, pp. 721–730, 2007.

[22] H. Ru Tseng, R. H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *IEEE Global Telecommunications Conference (GLOBECOM'07)*, pp. 986–990, 2007.

[23] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in *IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'10)*, pp. 600–606, 2010.

[24] B. Vaidya, J. Silva, and J. J. P. C. Rodrigues, "Robust dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the 5th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet'09)*, pp. 88–91, 2009.

[25] R. Watro, D. Kong, S. F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: Securing sensor networks with public key technology," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04)*, pp. 59–64, 2004.

[26] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*, pp. 244–251, 2006.

[27] J. Yuan, C. Jiang, and Z. Jiang, "A biometric-based user authentication for wireless sensor networks," *Wuhan University Journal of Natural Sciences*, vol. 15, no. 3, pp. 272–276, 2010.

Tanmoy Maitra received his B.E. degree in computer science and engineering from Burdwan University, India in 2009 and his M.Tech degree in computer science and engineering from WBUT, India in 2013. Now, he is pursuing Ph.D from Jadavpur University, India. He has qualified GATE in computer science in 2011 and 2012 respectively. He has published few international journal papers on remote user authentication system. His research interest includes wireless sensor networks and applied cryptology.

Ruhul Amin received his B.Tech and M.Tech degree from West Bengal University of Technology, India in computer science and engineering department in 2009 and 2013 respectively. Now, he is pursuing Ph.D from Indian Schools of Mines University, India. He has qualified GATE 2011 in computer science. He has published few international journal papers on remote user authentication system. His research interest includes remote user authentication and security in wireless sensor network.

Dr. Debasis Giri is presently Professor in the Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia-721657, India. He received his Ph. D on Cryptanalysis and Improvement of Protocols for Digital Signature, Smart-Card Authentication and Access Control from Indian Institute of Technology, Kharagpur 721 302, India in 2009. He did his masters (M. Tech and M. Sc) both from Indian Institute of Technology, Kharagpur in 2001 and 1998 respectively. He has tenth All India Rank with percentile score 98.42 in the Graduate Aptitude Test in Engineering (GATE) Examination in 1999. Dr. Giri has published more than 30 technical papers in several international journals/proceedings. He taught several courses such as Discrete Mathematics, Cryptography, Information Security, Coding Theory and Advanced Algorithms etc. His current research interests include cryptography, Network security, Security in Wireless Sensor Networks and Security in VANETs. Further, he is Editorial Board Member and Reviewer of many reputed International Journals. He is also Program Committee member of many International Conferences.

Dr. P. D. Srivastava has joined the Department of Mathematics, Indian Institute of Technology, Kharagpur as faculty in the year 1980 and became Professor in 1998. Dr. Srivastava has a very bright academic career. He has obtained his B.Sc., M.Sc. degree from Kanpur university in the year 1973 & 1975 respectively and Ph.D from I.I.T. Kanpur in the year 1980. Dr. Srivastava is not only an established researcher in his area but also a teacher par excellence. His style of lecture presentation and full command on the subject impress the students, which is reflected by the students in "Students' Profile

Forms" (teaching Assessment by the Students. During his 34 years teaching career, he taught several courses such as Functional Analysis, Topology, Numerical Analysis, Measure Theory, Real Analysis, Complex Analysis, Calculus etc. to undergraduate and postgraduate students. Besides teaching, Professor Srivastava is equally devoted to research Approximately 51 Papers published in very good and reputed journals of mathematics, are credited to his account. He has supervised 10 research scholars for Ph.D. Degree in mathematics and one for PDF. Various universities have invited him for Lectures/Key note address in the conferences. Various universities invite him as an expert in the Faculty selection as well as an expert to adjudicate the Ph.D. theses. He is also reviewer for the Mathematical Reviews as well as Paper referee for many journals.