Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 348783, 8 pages
http://dx.doi.org/10.1155/2013/348783

*Research Article*

# Improved Security Patch on Secure Communication among Cell Phones and Sensor Networks

**Ndibanje Bruce,[1] Tae-Yong Kim,[2] and Hoon Jae Lee[2]**

[1] *Department of Ubiquitous IT, Graduate School of Dongseo University, Sasang-Gu, Busan 617-716, Republic of Korea*
[2] *Division of Computer and Engineering, Dongseo University, Sasang-Gu, Busan 617-716, Republic of Korea*

Correspondence should be addressed to Tae-Yong Kim; tykimw2k@gdsu.dongseo.ac.kr

Received 31 August 2012; Revised 28 March 2013; Accepted 28 March 2013

Academic Editor: Sabah Mohammed



The communication between cell phones and sensor networks involves strong user authentication protocols to ensure the data and network security. Generally, in order to obtain the relevant information, cell phones interact with sensor networks via gateways. In 2009, according to Arjan Durresi and Vamsi Paruchuri scheme, this unique ability is used to provide better authentication and security protocols that can be used to establish secure communications among cell phones and sensor networks. In this paper, we show that their scheme is vulnerable to known attacks such as man-in-the-middle attack and reply attack, and it does not provide mutual authentication between gateway node and cell phone. In addition, it does not establish session key after the authentication phase. To fill this security gap, we proposed security patches and improvements, which overcome the weak features in the scheme of Arjan Durresi and Vamsi Paruchuri. Finally, we came out with results which show that our improved security patch establishes trust between the cell phone and gateway in the form of mutual authentication and provides the session key establishment after the authentication phase.

## 1. Introduction

With the recent advances in information and communication technology, the wireless sensor networks (WSNs) have attracted an increasing interest from researchers due to its ubiquitous nature. Wireless sensor networks (WSNs) are normally deployed in an unattended environment to collect the data which are transmitted to the base-station traversing some nodes via RF signals and routing schemes. In general, most of the queries in WSN applications are issued at the points of base stations or gateway (GW) nodes of the network. However, due to the wireless nature of sensor node it may be possible that a user can access sensor data directly without involving the gateway. Thus, user authentication is a primary concern in this resource-constrained environment before accessing data from the sensor/gateway nodes. WSNs are widely used in areas such as military, battlefield, homeland security, healthcare monitoring, agriculture and cropping, manufacturing, and measurement of seismic activity, and so forth. Every sensor node has some level of computing power, limited storage, and a small communication module to communicate with the outside world over an ad hoc wireless network [1]. Thus far authentication protocols schemes have been proposed on the link layer [2–5] and the network layer [6], and they provide sufficient security in the wireless sensor networks. Meanwhile, protocols based on user authentication on the application layer in [7–10] have been proposed where the secrets are stored into the gateway node or base station. In that case, when a user wants to access data through the gateway node or base station, he is authenticated those protocols. Through cellular network, user can access gateway of wireless sensor networks and get the data he wants to access. Cell phones are ubiquitous and have a low power transceiver that communicates with the base stations that are typically located on a distance of a few miles. There are many applications which would greatly benefit from using cell phones in the ad hoc mode. Collecting data from a gateway by a cell phone, needs an authentication protocols are needed to prevent a malicious cell phone user from misguiding other users [11].

In 2009, Durresi and Paruchuri [12] proposed architecture among the cellular network and wireless sensor networks with protocols to establish secure communication. According to their scheme, the gateways are connected to an authentication server (AS), and each sensor network has its own AS in charge of their security. A central server (CS) that interacts with all ASs and cell phones is required. The CSs communicate with cell phones through the existing cellular network only to exchange control and security information. The data communication between cell phones and sensor networks (gateways) is done through ad hoc channels. The control of the security across all the sensor networks is done by the CS, and it could be distributed. To utilize the advantages of both cell phones and sensor nodes, the use of gateways nodes was proposed. These nodes act as sinks for sensor networks to obtain and aggregate the relevant information sensed by the sensor network. Gateways act also as intermediates through which the cell phones get information from sensor networks. Cell phones can communicate with cellular network and sensor networks at the same time. They claimed that this unique ability is used to provide better authentication and security.

Unfortunately, this paper finds that Arjan et al.'s scheme is susceptible to information leakage attack, to man-in-the-middle attack, reply attack, and no mutual authentication between the cell phone and the gateway, and no session key is established between the cell phone and the gateway node at the end of the authentication phase.

The rest of the paper is structured as follows. Section 2 briefly reviews Arjan et al.'s schemes. Section 3 elaborates on the weaknesses and security pitfalls of his scheme. Section 4, presents our improved security patch over Arjan et al.'s scheme. Section 5 reveals the performance analysis of the presented scheme and Section 6 concludes this paper.

## 2. Review of Arjan et al.'s Scheme

In this section, we review Arjan et al.'s schemes. The first scheme uses asymmetric key cryptography, whereas the other scheme use symmetric key cryptography between cell phones and gateways.

*2.1. Review on Using Secure Infrastructure and Asymmetric Cryptography Scheme.* The first scheme of Arjan et al. is using the identity-based cryptography (IBC) to provide a secure connectivity. According to their architecture, each sensor node has a private key generator (PKG) which is part of the authentication server. The notations used throughout this paper are given in Table 1.

The system model of Arjan et al.'s architecture is defined by different components as follows:

(i) cell phones (CP)

(ii) cellular base station (CBS)

(iii) central server (CS)

(iv) authentication server (AS)

(v) sensor networks

(vi) gateways ($G$).

Table 1: Notations and descriptions.

| Notations | Descriptions |
|---|---|
| $S_{\mathrm{ID}}$ | Session identity |
| $\mathrm{ID}_G$ | ID of the gateway |
| $\mathrm{ID}_N$ | ID of the sensor network |
| $K_S$ | Session key |
| EK (M) | Encryption of message M with key K |
| SK | Secret key |
| PK | Public key |
| $\mathrm{SK}_{\mathrm{PKG}}$ | Secret key of the PKG |
| $\mathrm{PK}_{\mathrm{PKG}}$ | Public key of the PKG |

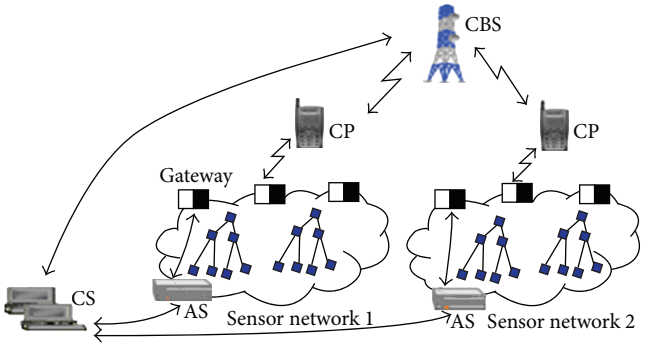


Figure 1: Arjan et al. network architecture.

The proposed architecture by Arjan et al. is shown in Figure 1, and they claimed that it supports secure communication among cell phones and sensor networks.

In Figure 1, the CP does not communicate directly with the sensor network. It has first to be requested from the CS a $\mathrm{PK}_{\mathrm{PKG}}$ of that particular sensor network. The CS generates the $S_{\mathrm{ID}}$ for the CP and also requests to the AS of the sensor network a $\mathrm{SK}_{\mathrm{PKG}}$ corresponding to that $S_{\mathrm{ID}}$ of the CP. The CS then transmits the $S_{\mathrm{ID}}$, $\mathrm{PK}_{\mathrm{PKG}}$ and the $\mathrm{SK}_{\mathrm{PKG}}$ to the CP through the cellular network. The CP will use this triplet to communicate with the sensor network via the gateway.

Initially the CP interacts with the CBS, and after the CP is authenticated by the BCS, a session key $K_S$ is established to secure their communication [13, 14]. Once the CP wants to communicate with sensor network through the gateway, it sends a request to the CS via the cellular network. CP sends the $\mathrm{ID}_N$ of the sensor network and the $\mathrm{ID}_G$ of the gateway encrypted with $K_S$ as follows:

$$\mathrm{CP} \longrightarrow \mathrm{CBS} : \left\langle E_{K_S} \left[\mathrm{ID}_N \parallel \mathrm{ID}_G\right]\right\rangle. \tag{1}$$

The CS interacts with the AS of the given sensor network in the aim to obtain the $\mathrm{SK}_{\mathrm{SID}}$ corresponding to the $S_{\mathrm{ID}}$ of the CP. The message is sent to the CP via the cellular network as follows:

$$\mathrm{CBS} \longrightarrow \mathrm{CP} : \left\langle E_{K_S} \left[\mathrm{ID}_N \parallel \mathrm{ID}_G \parallel S_{\mathrm{ID}} \parallel \mathrm{SK}_{\mathrm{SID}} \parallel \mathrm{PK}_{\mathrm{PKG}}\right]\right\rangle. \tag{2}$$

The communication between the cell phone and the gateway is done through ad hoc channels. To communicate with the

given sensor network the CP sends a query to the gateway $G$ using his $S_{\mathrm{ID}}$ and sign with its own private key. The CP encrypts the query with the public key of $G$ generated using the $\mathrm{ID}_G$ and $\mathrm{PK}_{\mathrm{PKG}}$.

$$\mathrm{CP} \longrightarrow G : S_{\mathrm{ID}} \parallel E_{\mathrm{SK}_{\mathrm{SID}}} \left[E_{\mathrm{PKG}} \left[\mathrm{Query} \parallel \mathrm{ID}_N\right]\right]. \quad (3)$$

Finally, the gateway responds to the message of the CP; the gateway encrypts the message with public key of CP and signs with its secret key as follows:

$$G \longrightarrow \mathrm{CP} : \mathrm{ID}_G \parallel E_{\mathrm{SK}_G} \left[E_{\mathrm{PKSID}} \left[\mathrm{Query} \parallel \mathrm{Reply} \parallel \mathrm{ID}_N\right]\right]. \quad (4)$$

*2.2. Review on Using Secure Infrastructure and Symmetric Cryptography Scheme.* This scheme uses symmetric cryptography to provide secure links between CP and gateways. The CP shares keys with gateways. If the cell phone wants to communicate with a sensor network, it sends the $\mathrm{ID}_N$ of that sensor network through the cellular network to the CS.

The CS interacts with AS of that sensor network to obtain a set of secrets key for the CP. The AS also distributes each key of the set to some gateways. The CP broadcasts its $S_{\mathrm{ID}}$ when wants to communicate with the gateways. Only the gateways with shared keys interact with the CP. When a CP wants to communicate with the sensor network, it sends the $\mathrm{ID}_N$ encrypted with the key shared with the CBS as follows:

$$\mathrm{CP} \longrightarrow \mathrm{CBS}: \left\langle E_{K_S} \left[\mathrm{ID}_N\right]\right\rangle. \quad (5)$$

The message is sent through the CBS to the CS which interacts with the appropriate AS, and then the AS provides a set of privates keys ($S$) to the CP as follows:

$$\mathrm{CBS} \longrightarrow \mathrm{CP} : \left\langle E_{K_S} \left[\mathrm{ID}_N \parallel S_{\mathrm{ID}} \parallel S\right]\right\rangle. \quad (6)$$

Now, the CP has the $S_{\mathrm{ID}}$ and secrets keys to be authenticated to the gateways. The CP broadcasts its $S_{\mathrm{ID}}$ to the sensor network in (7). Thus, only the gateways with the shared pairwise key interact with CP after authentication procedure as follows:

$$\mathrm{CP} \longrightarrow \mathrm{ALL} : \left\langle S_{\mathrm{ID}}\right\rangle, \quad (7)$$

$$G \longrightarrow \mathrm{CP} : \left\langle S_{\mathrm{ID}}, \mathrm{ID}_G, E_{K_c} \left[\mathrm{ID}_G \parallel \mathrm{RAND}\right]\right\rangle, \quad (8)$$

$$\mathrm{CP} \longrightarrow G : \left\langle S_{\mathrm{ID}}, \mathrm{ID}_G, E_{K_c} \left[\mathrm{ID}_G \parallel f\,(\mathrm{RAND})\right]\right\rangle. \quad (9)$$

The gateway with the shared pairwise key sends a random challenge with its ID encrypted with the key $K_c$ shared with the gateway to the CP in (8), and the CP responds to the challenge in (9) for the authentication purpose by the gateway.

## 3. Cryptanalysis and Weakness of Arjan et al.'s Schemes

Initially the cell phone interacts with the cellular base station. The cell phone is authenticated by the cellular base station and a session key $K_S$ is established to secure the communication between the cell phone and the cellular base station. Arjan et al. claimed that the fact that the $S_{\mathrm{ID}}$ and $\mathrm{SK}_{\mathrm{SID}}$ are obtained via the cellular network benefits, the scheme strong and secure authentication.

However, their scheme presents a gap of weakness security as follows.

(i) *Information leakage attack*: as an alternative, the attacker can perform a man-in-the-middle attack [15] (enter between the cell phone and the cellular base station by using a malicious cell phone and fake cellular base station), such that all the messages pass through the attacker. During the authentication phase between the cell phone and the cellular base station, only the cell phone is authenticated to the cellular base station while there is no mechanism to authenticate the cellular base station to the cell phone. Then, any adversary can perform the man-in-the-middle attack.

(ii) *Replay attack*: the attack occurs when an adversary intercepts the message (3) and (7) (i.e., if the attacker accesses the SIM card of the legitimate user) and replays it, he might impersonate the gateway to be a real cell phone using an authenticated session key unless the gateway remembers indefinitely all previous sessions keys used with the cell phone. Here, Arjan et al.'s scheme, does not provide any mechanism to prevent the re-use of olds sessions keys. The gateway responds to the adversary's query, and CP-adversary, who is an adversary and not a legitimate user of the sensor network system, finally, he enjoys the resources as an authorized user without being a member of the system.

(iii) *Session-key establishment:* Arjan et al.'s scheme does not establish the session key between the cell phone and the gateway after authentication phase. After successful user authentication, the involved parties should establish a session key, so that subsequent messages could transmit securely. Thus, Arjan et al.'s scheme fails to establish the session key after user authentication phase.

## 4. Proposed Security Improvements

*4.1. Protection against Man-in-the-Middle-Attack.* To resist to the man-in-the-middle attack, we propose to use 3G instead of 2–2.5G networks. In GSM authentication only user authentication to the network is provided. To come out this weakness we propose to use 3G network where [16] both network and cell phone can authenticate each other. Thus the mutual authentication is well performed and can avoid against a man-in-the-middle attack.

*4.2. Protection against Reply Attack with Mutual Authentication between Cell Phone and Gateway.* It was identified in Section 3(ii) that there is a possibility of a replay attack in Arjan et al.'s scheme. The reason of the possibility of the replay attack is due to the absence of mechanism to prevent the re-use of olds sessions keys. In the case of an adversary can capture the messages (3) and (7), can replay them and access

to the resources of the sensor networks. To overcome to this security flaw, we propose to use nonce and timestamp for mutual authentication between cell phone and gateway. Arjan et al.'s scheme can be amended by Table 2.

Before detailed discussion of the proposed scheme, some assumptions are made and are not supposed to be violated while executing the scheme. The assumptions are mentioned below.

(1) The CP is registered to the AS via CBS using 3G technology. The AS assigns the $S_{\text{ID}}$ and the corresponding secret key to the CP via the same CBS. We assume that all the clients and service providers are supposed to be honest in the registration phase.

(2) Using a secure communication channel, the AS assigns ID and private key to each gateway.

The authentication phase (AP) is invoked when the cell phone wants to login the WSN and access data from the gateway with the followings steps.

#### 4.2.1. Using Secure Infrastructure and Asymmetric Cryptography Scheme

*AP-1.* The cell phone generates a secret number $X_{\text{cp}}$ and calculates $V_{\text{cp}}$ as follows: $V_{\text{cp}} = g^{h(X_{\text{cp}}||N_{\text{cp}})} \bmod p$ and sends to $G$. Here $N_{\text{cp}}$ is the nonce of the cell phone. To send the query $Q$ to the gateway, the cell phone encrypts it with the public key of the gateway and signs it with its own private key: $Q = E_{\text{SK}_{\text{SID}}}[S_{\text{ID}} \| T_{\text{cp}} \| [E_{\text{PKG}}(\text{Query} \| \text{ID}_N)]]$. $T_{\text{cp}}$ is the timestamp of the cell phone. The CP sends $V_{\text{cp}}$ and $Q$ in the message (3) to the gateway.

*AP-2.* Upon receiving message (3) from the cell phone, the gateway decrypts it and performs the followings actions.

(1) The gateway $G$ validates the time $T_{\text{cp}}$ and check if $(T_g - T_{\text{cp}}) \geq \Delta T$. If yes, then abort if not continues with the next step. Here, $T_g$ is the current timestamp of the gateway and $\Delta T$ is the defined time interval for the transmission delay.

(2) The gateway verify if $S_{\text{ID}} = S'_{\text{ID}}$ if yes, then the gateway node considers that, this is a legitimate user and proceeds to the next step; otherwise, it terminates the operations.

(3) The gateway generates a secret number $L_g$ and with $V_{\text{cp}}$, $G$ calculates the session key $S_{\text{ESK}} = V_{\text{cp}}^{L_g} \bmod p$. Subsequently, the gateway generates the nonce $N_g$ then calculates $V_g$ as follows: $V_g = g^{h(L_g||N_g)} \bmod p$ and sends to cell phone $B$. Here, $B = E_{\text{SESK}}(V_g \| N_{\text{cp}})$. To respond to the query, the $G$ encrypts it with the public key of the CP and signs it with its private key. $R = E_{\text{SKG}}[\text{ID}_G \| S_{\text{ID}} \| T_g \| E_{\text{PKSID}}[\text{Query} \| \text{Reply} \| \text{ID}_N]]$. The $G$ sends $B$ and $R$ in message (4) to the cell phone.

*AP-3.* After receiving the reply message (4) from the $G$, the CP performs the following actions.

Table 2: Notations and descriptions.

| Notations | Descriptions |
|---|---|
| $N_{\text{cp}}$ | Nonce generated by cell phone |
| $T_{\text{cp}}$ | Timestamp for cell phone |
| $X_{\text{cp}}$ | Cell phone's secret number |
| $V_{\text{cp}}$ | Value of Diffie-Hellman function for cell phone |
| $V_g$ | Value of Diffie-Hellman function for gateway |
| $T_g$ | Timestamp of gateway |
| $N_g$ | Nonce generated by the gateway |
| $L_g$ | Gateway's secret number |
| $S_{\text{ESK}}$ | Session key |
| $h(\cdot)$ | Cryptographic hash function, for example, SHA1 and SHA2 |
| $\|$ | Denotes concatenation operation |
| $p$ | A large prime number |
| $g$ | Primitive element in the Galois field GF ($p$) |

(1) checks if $(T_{\text{cp}} - T_g) \leq \Delta T$, then CP proceeds to the next step; otherwise, the step is terminated. Here $\Delta T$ shows the expected time interval for the transmission delay.

(2) The CP decrypts the message with its private key and check if $N'_{\text{cp}} = N_{\text{cp}}$, $\text{ID}'_G = \text{ID}_G$ if yes, then continues to the next step if not abort it.

(3) The CP obtains $V_g$ and calculates the session key $S_{\text{ESK}}$ using the followings: $S_{\text{ESK}} = V_g^{X_{\text{cp}}} \bmod p$.

(4) Now, the CP sends the last message $M_5$, to acknowledge the session key from the gateway: $M_5 = E_{\text{SESK}}(I \| V_{\text{cp}})$. Here, $I = h((\text{ID}_G) \| N_g)$.

*AP-4.* While receiving the message $M_5$, the gateway performs the following.

(1) It computes the session key and decrypts the sub message, obtains $N'_g$ and $V'_{\text{cp}}$. The gateway checks if $N'_g = N_g$, $V'_{\text{cp}} = V_{\text{cp}}$, if the conditions are true the gateway believes that the CP is a legitimate one otherwise not.

(2) Furthermore, the cell phone and the gateway node share the session key $S_{\text{ESK}}$ to perform subsequent operation during a session and the establishment of the session key terminates the authentication phase.

#### 4.2.2. Using Secure Infrastructure and Symmetric Cryptography Scheme.

To enhance to security in Arjan et al.'s scheme using symmetric cryptography, the same assumptions are taken in considerations. The authentication phase (AP) is invoked when the cell phone wants to login the WSN and access data from the gateway with the followings steps.

*AP-1.* CP generates a secret number $X_{\text{cp}}$ calculates $I$ and as follows: $I = g^{h(N_{\text{cp}}||X_{\text{cp}})} \bmod p$. $N_{\text{cp}}$ is the nonce of the cell phone. From the message (10), the cell phone broadcasts its

$S_{\mathrm{ID}}$ with the value of $B$ to all the gateways. Here, $B = h(I \| T_{\mathrm{cp}})$, and $T_{\mathrm{cp}}$ is the timestamp of cell phone.

$$\mathrm{CP} \longrightarrow \mathrm{ALL} : \left\langle E_{K_c} \left[ S_{\mathrm{ID}}, B \right] \right\rangle. \tag{10}$$

*AP-2*. The gateway which shares the pairwise key will interact with the cell phone with the actions below.

(1) The gateway $G$ checks if $(T_g - T_{\mathrm{cp}}) \geq \Delta T$; if yes, then aborts it if not continues with the next step.

(2) The gateway generates a secret number $L_g$ and calculates $D$ using the following: $D = g^{h(L_g \| N_g)} \bmod p$. G sends in message (11) a random challenge to the cell phone encryption with the value of $J$. Here, $J = h(D \| T_g)$

$$G \longrightarrow \mathrm{CP} : \left\langle S_{\mathrm{ID}}, \mathrm{ID}_G, E_{K_c} \left[ J \parallel N_{\mathrm{cp}} \parallel \mathrm{ID}_G \parallel f \ \ (\mathrm{RAND}) \right] \right\rangle. \tag{11}$$

*AP-3*. While receiving the message (11), the CP decrypts the message and performs the followings.

(1) The CP validates the time $T_g$ and check if $(T_{\mathrm{cp}} - T_g) \geq \Delta T$; if yes, then abort it, if not continues with the next step.

(2) The CP verifies if $N'_{\mathrm{cp}} = N_{\mathrm{cp}}$ if yes, then, continues to the next step if not abort.

(3) Then, the cell phone calculates the session key to respond to the challenge $S_{\mathrm{ESK}} = h(h(\mathrm{SID}) \| N_{\mathrm{cp}} \| \mathrm{ID}_G \| N_g)$. Now, the CP sends through message (12) the response,

$$\mathrm{CP} \longrightarrow G : E_{K_c} \left( S_{\mathrm{ESK}} \parallel f\,(\mathrm{RAND}) \right). \tag{12}$$

*AP-4*. Upon receiving message (12) from the cell phone, the gateway computes the message and decrypts the sub message to retrieve the session key and check if $\mathrm{ID}_G = \mathrm{ID}_G$, $N'_g = N_g$, if yes the gateway believes that the CP is a legitimate one otherwise not.

Finally, the cell phone and the gateway shares the session key $S_{\mathrm{ESK}}$ to perform subsequent operation during a session and the establishment of the session key terminates the authentication phase.

## 5. Performance Analysis of Proposed Scheme

In this section, we summarize security features and performance analysis of our proposed scheme and compare its security features and robustness with the scheme of Arjan et al. The performance analysis demonstrates that our scheme is more secure and robust than the scheme of [12], and achieves more security features, which were not considered in the aforementioned scheme. In addition a comparison with recent secure communication in WSN with our proposed protocol is done for the sufficient qualities.

*5.1. Security Analysis*

(1) *Mutual authentication between the CP and the CBS*: our scheme proposes to use 3G instead of 2–2.5G networks. The GSM authentication mechanism is only one way; therefore, the user is not given the assurance that he has established a connection with an authentic serving network. With 3G technology, there is the assurance that authentication information and keys are not being re-used (key freshness).

(2) *Mutual authentication between the CP and the G*: in message (3) AP-2, the gateway verifies if the ID of the CP is the real one got from the AS, also the cell phone checks if $N'_{\mathrm{cp}} = N_{\mathrm{cp}}$ in AP-3 of message (4). By the end, the gateway verifies if $N'_g = N_g$, $V'_{\mathrm{cp}} = V_{\mathrm{cp}}$ and both of them are mutually authenticated. In the case of symmetric cryptographic scheme, the same analyses are applied in message, (11) and (12).

(3) *Man-in-the middle attack*: in message (3), if an attacker intercepts $V_{\mathrm{cp}}$, he cannot calculate the session key without knowing the secret number $L_g$ stored in the gateway. Even if the attacker could calculate a session key, the cell phone should reject the request because in AP-3 of message (4), the cell phone will check if $N'_{\mathrm{cp}} = N_{\mathrm{cp}}$, $\mathrm{ID}'_G = \mathrm{ID}_G$. The same analyses are applied in message (12) in the case of symmetric cryptographic scheme.

(4) *Reply attack*: in this case, an attacker can steal the SIM card of the user of the cell phone and puts it in its cell phone. In this case, the attacker can use the $S_{\mathrm{ID}}$ from the AS and try to access the WSN. Our scheme is timestamp based and nonce based. In the timestamp-based scheme, if an adversary wants to replay the mutual authentication message to the gateway or cell phone, then $G$ or CP would reject it, because they validate the timestamp ($T_{\mathrm{cp}}$ or $T_g$) and if it is expired, they terminates further operations. On the other hand, in the nonce-based authentication scheme, if an intruder replays the mutual authentication message to the $G$ or CP would reject it because the nonce ($N_{\mathrm{cp}}$ or $N_g$) is randomly generated and expires after the session is terminated or expired.

(5) *Session key establishment*: a session key, $S_{\mathrm{ESK}}$ is established between the cell phone and the gateway after authentication process. This key is different in each session and cannot be replayed after the session expires.

As illustrated in Table 3, it is obvious that the proposed scheme is a secure user authentication protocol and provides more security services than Arjan et al.'s scheme.

*5.2. Performance Comparison among Existing Protocols.* Recent researches have been conducted in WSN communication, and results show that they are efficiently secured in terms of computation cost and communication cost. Different existing schemes [17–23] have been analyzed in their

Table 3: Functionality comparison.

| | Arjan et al.'s scheme [12] | Our scheme |
|---|---|---|
| (A) Security features | | |
| Mutual authentication between CP and CBS | No | Yes |
| Mutual authentication between CP and G | No | Yes |
| Secure session key agreement | No | Yes |
| Avoid replay attack | No | Yes |
| Avoid man-in-the middle attack | No | Yes |
| (B) Computation type | | |
| Symmetric en/decryption | Yes | Yes |
| Asymmetric en/decryption | Yes | Yes |
| Authenticator function | No | Yes |

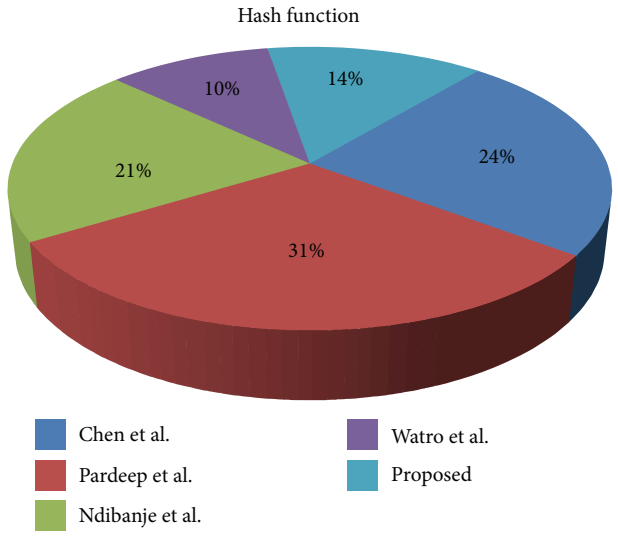


Figure 2: Total time complexity (hash function).

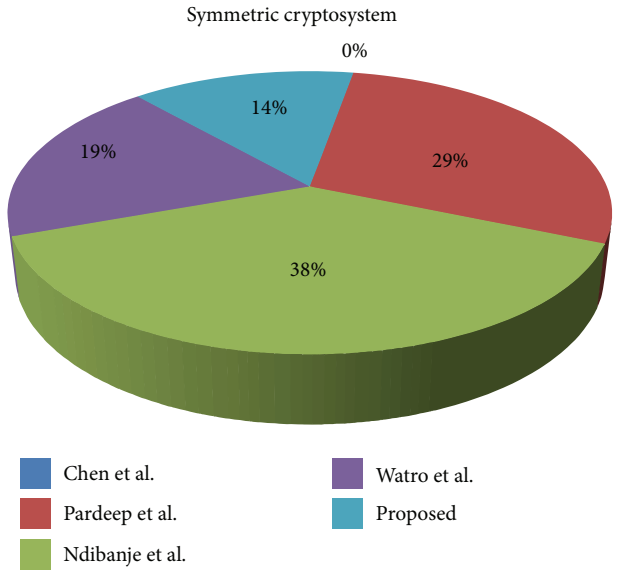


Figure 3: Total computation cost (symmetric cryptosystem).

communication protocols for the whole communication and confirmation of all entities (i.e., *user*, *gateway*, and *sensor*). In some cases all entities exchange messages or some of them only can exchange messages. In all cases, we carefully took in consideration the behavior of each protocol so that we can see how our protocol is efficient. Let us set $T_h$ as the computation time, and let us set $T_s$ as time for symmetric cryptosystem (the private/public key computation time), as referred in [17–23]. The comparison result is given in Table 4. The purpose of the performance analysis is to minimize the power consumption of the sensor node as it is a primary concern in this resource-constrained environment. In the Arjan et al.'s scheme, they did not deal with communication between sensor node and user, and we have kept this architecture because we found that it is the best one in term of sensor node with less power consumption. Thus, there is no computation activity among cell phone user, and sensor nodes. The performance comparison results of our proposed protocol and related ones are illustrated in details in Table 4.

The results from Table 4 show that the proposed protocol in the authentication phase (with authentication verification and mutual authentication) requires $6T_H$ hush function and $3T_S$ for symmetric cryptosystem, whereas in others protocols [17–19] and [20] need $9T_H + 6T_S + 2\text{MAC}$, $7T_H$, $6T_H + 8T_S$ and $2T_H + 4T_S$; respectively, for whole authentication phase. From this analysis, we can see that for time complexity, our protocol needs $3T_S$ to achieve the calculation of public/private key, whereas others needs more for that operation. The good reason behind that is the less power consumption of the devices. Regarding the time complexity, our protocol requires $6T_H$ for hush function calculation ($9T_H$, $7T_H + 6T_S$) and $2T_H$ for others. Analyzing the performance of the proposed protocol in term of communication cost, the result from Table 4 reveres that our protocol requires 3 messages exchange for the whole communication and confirmation of all entities. Watro et al.'s protocol needs only 2 messages exchange because their protocol does not deal with gateway node communication. The user communicates straight with the sensor node. Even if our protocol has one more message of message exchanges as that of Watro et al.'s and same number of message exchanges in [19], the message size (the content of the messages exchanges) of ours is smaller than them. Hence, the proposed protocol has a valuable computation cost among the compared protocols.

Figures 2 and 3 show the total time complexity of hash function and computation cost of cryptosystem respectively, while Figure 4 describes the total messages exchanges for the whole communication and confirmation of all entities used in the protocols aforementioned.

## 6. Conclusion

In real time, as a cell phone user can access data from gateway trough wireless sensor network; it is imperative to control data accessibility with strong user authentication protocols.

Table 4: Performance comparison with related protocols.

| Related protocols | Protocol: authentication (verification and mutual authentication) | | | Comm cost |
|---|---|---|---|---|
| | User | G-node | S-node | |
| Chen and Shih [17] | $1T_H$ | $5T_H$ | $1T_H$ | 4 ME |
| Kumar et al. [18] | $4T_H + 2T_S$ | $4T_H + 2T_S$ + 1MAC | $1T_H + 2T_S$ + 1MAC | 4 ME |
| Bruce and Lee [19] | $4T_H + 4T_S$ | $2T_H + 4T_S$ | N/A | 3 ME |
| Watro et al. [20] | $1T_H + 2T_S$ | N/A | $1T_H + 2T_S$ | 2 ME |
| Proposed | $4T_H + 2T_S$ | $2T_H + 1T_S$ | N/A | 3 ME |

N/A: not applicable; ME: messages exchanges.

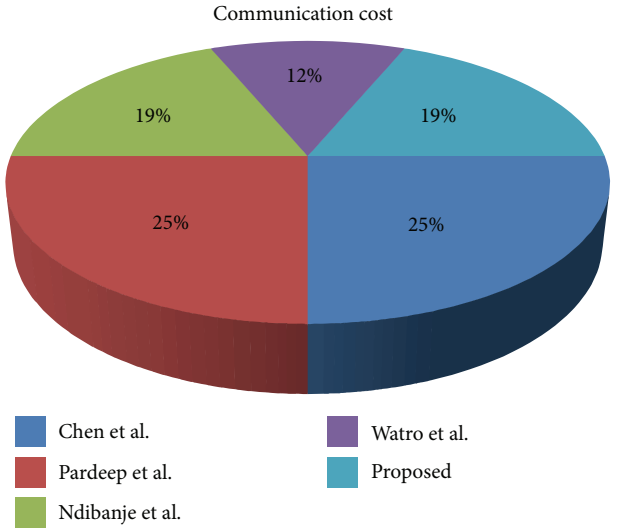


Figure 4: Total messages exchanges for whole communication.

In this regard, we have proposed enhancements to the scheme of Arjan et al. which suffers from Information leakage attack, does not provide mutual authentication between gateway node and cell phone, not able to establish session key after the authentication phase and it is susceptible to reply attack. To remedy the aforementioned flaws, we have proposed security patches and improvements, that overcome the weak features of Arjan et al.'s scheme and can be incorporated in their scheme for a more secure and robust authentication protocol in WSNs. Hence, through analysis, we came out with the conclusion that in our enhanced proposed improvement, the cell phone authenticates the gateway and both parties can trust on the authenticity of each other.

## Acknowledgments

This work was supported by Dongseo University, "Dongseo Frontier Project" Research Fund of 2009. It was also supported by the National Research Foundation (NRF) 2012 Project (Grant no. 2012-0008447).

## References

[1] E. H. Callaway, *Wireless Sensor Networks, Architectures and Protocols*, Auerbach Publications, Taylor & Francis Group, Boca Raton, Fla, USA, 2003.

[2] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MOBBICOM '01)*, pp. 189–199, Rome, Italy, July 2001.

[3] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 162–175, Baltimore, Md, USA, November 2004.

[4] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: a secure sensor network communication architecture," in *Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN '07)*, pp. 479–488, Cambridge, Mass, USA, April 2007.

[5] P. Kumar, S. Cho, D. S. Lee, Y. D. Lee, and H. J. Lee, "TriSec: a secure data framework for wireless sensor networks using authenticated encryption," *International Journal of Maritime Information and Communication Sciences*, vol. 8, pp. 129–135, 2010.

[6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[7] Z. Benenson, F. Gartner, and D. Kesdogan, "User authentication in sensor network (extended abstract)," in *Proceedings of the Workshop on Sensor Networks Informatik*, vol. 34, Jahrestagung der Gesellschaft fur Informatik, Ulm, Germany, September 2004.

[8] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authentication in sensor networks," in *Proceedings of the Workshop on Real-World Wireless Sensor Network (REALWSN '05)*, Stockholm, Sweden, June 2005.

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

[10] H. R. Tseng, R. H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '07)*, pp. 986–990, Washington, DC, USA, November 2007.

[11] L. Buttyán and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, 2003.

[12] A. Durresi and V. Paruchuri, "Secure communication among cell phones and sensor networks," in *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM '09)*, December 2009.

[13] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04)*, pp. 586–597, March 2004.

[14] A. Durresi, V. Bulusu, V. Paruchuri, M. Durresi, and R. Jain, "Key distribution in mobile heterogeneous sensor networks," in *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM '06)*, November-December 2006.

[15] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of GSM encrypted communication," *Journal of Cryptology*, vol. 21, no. 3, pp. 392–429, 2008.

[16] A. M. Mojtaba, A. M. Mostafa, and A. Shahbahrami, "Evaluation of security attacks on UMTS, authentication mechanism," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 4, no. 4, 2012.

[17] T. H. Chen and W. K. Shih, "A robust mutual authentication protocol for wireless sensor networks," *ETRI Journal*, vol. 32, no. 5, pp. 704–712, 2010.

[18] P. Kumar, A. J. Choudhury, M. Sain, S. G. Lee, and H. J. Lee, "RUASN: a robust user authentication framework for wireless sensor networks," *Sensors*, vol. 11, no. 5, pp. 5020–5046, 2011.

[19] N. Bruce and H. J. Lee, "A secure authentication protocol among mobile phone and wireless sensor networks," in *Proceedings of the 15th International Conference on Advanced Computing Technologies (ICACT '13)*, pp. 52–59, Phoenix Park, Republic of Korea, January 2013.

[20] 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 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, pp. 59–64, Washington, DC, USA, October 2004.

[21] H. R. Tseng, R. H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07)*, pp. 986–990, November 2007.

[22] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers & Security*, vol. 21, no. 4, pp. 372–375, 2002.

[23] T. H. Chen, H. C. Hsiang, and W. K. Shih, "Security enhancement on an improvement on two remote user authentication schemes using smart cards," *Future Generation Computer Systems*, vol. 27, no. 4, pp. 377–380, 2011.