

Article

## Cryptanalysis and Security Improvements of ‘Two-Factor User Authentication in Wireless Sensor Networks’

Muhammad Khurram Khan <sup>1,\*</sup> and Khaled Alghathbar <sup>1,2</sup>

<sup>1</sup> Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia

<sup>2</sup> Information Systems Department, College of Computer and Information Sciences, King Saud University, Saudi Arabia; E-Mail: kalghathbar@ksu.edu.sa

\* Author to whom correspondence should be addressed; E-Mail: mkhurram@ksu.edu.sa;  
Tel.: +966-1-4696457.

Received: 5 January 2010; in revised form: 4 March 2010 / Accepted: 12 March 2010 /

Published: 23 March 2010

---

**Abstract:** User authentication in wireless sensor networks (WSN) is a critical security issue due to their unattended and hostile deployment in the field. Since sensor nodes are equipped with limited computing power, storage, and communication modules; authenticating remote users in such resource-constrained environments is a paramount security concern. Recently, M.L. Das proposed a two-factor user authentication scheme in WSNs and claimed that his scheme is secure against different kinds of attack. However, in this paper, we show that the M.L. Das-scheme has some critical security pitfalls and cannot be recommended for real applications. We point out that in his scheme: users cannot change/update their passwords, it does not provide mutual authentication between gateway node and sensor node, and is vulnerable to gateway node bypassing attack and privileged-insider attack. To overcome the inherent security weaknesses of the M.L. Das-scheme, we propose improvements and security patches that attempt to fix the susceptibilities of his scheme. The proposed security improvements can be incorporated in the M.L. Das-scheme for achieving a more secure and robust two-factor user authentication in WSNs.

**Keywords:** authentication; wireless sensor network; security; smart card; cryptanalysis

---

## 1. Introduction

With the recent advances in communication technologies, wireless sensor networks (WSN) have emerged as a very active research avenue. WSNs have many common features with wireless ad hoc networks, and in several cases they are considered as a special case of them [1]. A WSN usually consists of a large number of autonomous sensor nodes, which are generally deployed in unattended environments. Each 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 [2]. WSNs are widely used, including in areas such as military, battlefield, homeland security, healthcare, environment monitoring, agriculture and cropping, manufacturing, *etc.*

Since the sensor network may operate in a hostile environment such as a military battlefield, security is critical. Robust techniques are needed to provide low-latency, survivable, and secure networks during the deployment of WSN. In addition, the network should be protected against intrusions and spoofing attacks [3]. Access control is an indispensable cryptographic primitive upon which other security primitives are built. A WSN should be smart enough to distinguish legitimate users from illegitimate users, resulting in the problem of user authentication [3]. If a WSN is deployed for a highly secure application, then the data collected within the sensor work is valuable and should only be given access to the registered or legitimate users. Benenson *et al.* first sketched the security issues of user authentication in WSN and introduced the notion of *n-authentication* [4]. Later on, Watro *et al.* proposed a TinyPK authentication protocol with public key cryptography that uses RSA and Diffie-Hellman algorithms [5], however, this protocol suffers from masquerade sensor node attack, in which an adversary can spoof the user.

In 2006, Wong *et al.* [6] proposed a light-weight dynamic user authentication scheme in WSN environment. They justified their scheme through security and cost analysis and discussed the implementation issues with the recommendations of using the security features of IEEE 802.15.4 MAC sublayer. Later, Tseng *et al.* [7] identified some security weaknesses in the scheme of Wong *et al.*, which prevent it from being implemented in real-life environments. They showed that Wong *et al.*'s scheme is not protected from replay and forgery attacks, passwords can easily be revealed by any of the sensor nodes, and users cannot freely change their passwords. To overcome these discrepancies, Tseng *et al.* proposed an enhanced scheme and claimed that their scheme not only retains the advantages of Wong *et al.*'s scheme, but provides: resistance to replay and forgery attacks, reduction of password leakage risk, and capability of changeable password with better efficiency [7]. Lately, T.H. Lee [8] also analyzed Wong *et al.*'s scheme and proposed two simple dynamic user authentication protocols that are variations of Wong *et al.*'s scheme. In his first protocol, T.H. Lee simplified the authentication process by reducing the computational load of sensor nodes while preserving the same security level of Wong *et al.*'s scheme. On the other hand, in his second protocol, T.H. Lee proposed a scheme in which an intruder cannot impersonate the gateway node to grant access to illegitimate users.

L.C. Ko [9] proved that while Tseng *et al.*'s scheme achieves several security measures above Wong *et al.*'s scheme, it is still insecure under a reasonable attack model [9]. L.C. Ko discussed that Tseng *et al.*'s scheme does not achieve mutual authentication between the Gateway node (*GW*) and the Sensor node (*SN*), and between the User (*U*) and the SN. Furthermore, L.C. Ko identified that an adversary can forge the communication message which is sent from sensor node to the gateway node.

Consequently, L.C. Ko proposed a modified scheme which attempts to overcome the aforementioned security pitfalls of Tseng *et al.*'s protocol and proved that his scheme has better security features than Tseng *et al.*'s scheme. [7]

Binod *et al.* [10] cryptanalyzed the authentication schemes of Wong *et al.* and Tseng *et al.* and proposed their improved scheme. Binod *et al.* showed that their scheme is more robust than previously published schemes and can withstand replay attack, forgery attack, man-in-the-middle attack and provides mutual authentication between login node and gateway node.

Recently, M.L. Das [11] proposed a two-factor user authentication scheme in WSNs. M.L. Das also identified that Wong *et al.*'s protocol is vulnerable to many logged-in users with the same login-id threat, that is, who has a valid user's password can easily login to the sensor network [11]. He also identified that Wong *et al.*'s protocol is susceptible to stolen-verifier attack, because the GW-node and login-node maintain the lookup table of all the registered users' credentials. Consequently, M.L. Das proposed his protocol to overcome the security flaws of Wong *et al.*'s scheme. His protocol uses the two factor authentication concept based on password and smart card and resists many logged-in users with the same login identity, stolen-verifier, guessing, replay, and impersonation attacks.

More recently, Nyang and Lee pointed out that the protocol of M.L. Das is vulnerable to offline password guessing attack, sensor node compromising attack, and does not protect query response messages by establishing a unique secure channel from sensor node to a user, which is an important way of serving a registered user in a secure and legitimate way [17]. Consequently, Nyang and Lee proposed their improved two-factor authentication protocol for WSNs, which attempts to overcome their identified discrepancies in the M.L. Das scheme.

However, in this paper, we identify that the M.L. Das-scheme is still not secure and vulnerable to several critical security attacks. In addition to the problems identified by Nyang and Lee, we show that the M.L. Das-scheme is defenseless against GW-node by-passing attack, does not provide mutual authentication between GW-node and sensor nodes, has the security threat of insider attack, and does not have provision for changing or updating passwords of registered users. To fix the aforementioned weaknesses of the M.L. Das-scheme, we propose security improvements in our paper. Our enhanced security patch contains secure features of changing or updating passwords of users, provides protection against insider attack, overcomes the GW-node bypassing attack, and provides mutual authentication between GW-node and sensor node. The proposed security improvements can easily be incorporated into the M.L. Das-scheme to take the benefit of more secure and robust two-factor user authentication in WSNs.

The rest of the paper is organized as follows; Section 2 briefly reviews the M.L. Das-scheme, Section 3 elaborates on the weaknesses and security pitfalls of his scheme, Section 4 presents our proposed security patch, improvements and analysis over the M.L. Das-scheme, Section 5 reveals the performance analysis of the presented scheme, and finally, Section 6 concludes this paper.

## 2. Review of the M.L. Das-Scheme

In this section, we briefly review user the authentication scheme of M.L. Das, which is divided into two phases, namely the registration phase and the authentication phase.

### 2.1. Registration Phase

When a user  $U_i$  wants to perform registration with the WSN, he submits his  $ID_i$  and  $pw_i$  to the Gateway node (GW-node) in a secure manner. Upon receiving the registration request, the GW-node computes  $N_i = h(ID_i || pw_i) \oplus h(K)$ , where  $K$  is a symmetric key that is secure to the GW-node, and ‘||’ is a bit-wise concatenation operator. Now, the GW-node personalizes the smart card with the parameters  $h(\cdot), ID_i, N_i, h(pw_i)$  and  $x_a$ , where  $h(\cdot)$  is a one-way secure hash function and  $x_a$  is a secret value generated securely by the GW-node and stored in some designated sensor nodes before deploying the WSN. At the end of this phase,  $U_i$  gets his personalized smart card in a secure manner.

### 2.2. Authentication Phase

The authentication phase is invoked when  $U_i$  wants to login into WSN or access data from the network. This phase is further sub-divided into two phases, namely login and verification phases.

#### 1) Login Phase

In the login phase,  $U_i$  inserts his smart card into terminal and inputs  $ID_i$  and  $pw_i$ . The smart card validates the  $ID_i$  and  $pw_i$  with the stored values. If  $U_i$  is successfully authenticated, the smart card performs the following steps:

Step- L1: Computes  $DID_i = h(ID_i || pw_i) \oplus h(x_a || T)$ , where  $T$  is the current timestamp of  $U_i$  system

Step- L2: Computes  $C_i = h(N_i || x_a || T)$ , then send  $\langle DID_i, C_i, T \rangle$  to the GW-node

#### 2) Verification Phase

Upon receiving the login request  $\langle DID_i, C_i, T \rangle$  at time  $T^*$ , the GW-node authenticates  $U_i$  by the following steps:

Step-V1: Checks if  $(T^* - T) \leq \Delta T$  then GW-node proceeds to the next step, otherwise verification step is terminated. Here  $\Delta T$  shows the expected time interval for the transmission delay

Step-V2: Computes  $h(ID_i || pw_i)^* = DID_i \oplus h(x_a || T)$  and  $C_i^* = h((h(ID_i || pw_i)^* \oplus h(K)) || x_a || T)$

Step-V3: if  $C_i^* = C_i$  then GW-node accepts the login request; otherwise login request is rejected.

Step-V4: GW-node now sends a message  $\langle DID_i, A_i, T' \rangle$  to some nearest sensor  $S_n$  over a public channel to respond the query data what  $U_i$  is looking for, where the value of  $A_i$  is  $A_i = h(DID_i || S_n || x_a || T')$ , where  $T'$  is the current timestamp of the GW-node. Here, the value of  $A_i$  is used to ensure  $S_n$  that the message originally comes from the real GW-node.

Step-V5: After receiving the message  $\langle DID_i, A_i, T' \rangle$ , the  $S_n$  validates the timestamp. If the timestamp is within valid interval, then  $S_n$  computes  $h(DID_i || S_n || x_a || T')$  and checks whether it is equal to  $A_i$ . If this step is passed, then  $S_n$  responds to the  $U_i$ 's query.

### 3. Cryptanalysis and Security Pitfalls of the M.L. Das-Scheme

#### 3.1. GW-Node Bypassing Attack

In the M.L. Das-scheme, after performing the verification phase and accepting the login request of  $U_i$ , the GW-node sends an intimation message  $\langle DID_i, A_i, T' \rangle$  to some nearest sensor node  $S_n$  to inform about the successful login of  $U_i$ , and requests  $S_n$  to respond the query/data of  $U_i$ . Here,  $A_i$  is computed by  $A_i = h(DID_i || S_n || x_a || T')$ , where  $x_a$  is a secret parameter which is known to GW-node, sensor node and stored in the smart card of  $U_i$ .  $T'$  is the timestamp of GW-Node and  $DID_i$  is the dynamic ID of user, which is calculated by  $DID_i = h(ID_i || pw_i) \oplus h(x_a || T)$ . In the M.L. Das-scheme, the value of  $x_a$  is used to ensure  $S_n$  that  $A_i$  message is coming from the legitimate GW-node. Here, we assume that if the value of  $x_a$  is extracted from smart card of  $U_i$  by some means [12,13], then  $U_i$  himself or any adversary can login the  $S_n$  without going through the verification of GW-node, so Das *et al.*'s scheme is vulnerable to 'GW-node by-passing attack'. In the following, we show how this attack works on the M.L. Das-scheme:

- (i) Suppose an adversary or  $U_i$  himself computes a fake dynamic identity  $DID_a$  by using the extracted  $x_a$  from smart card  $DID_f = h(ID_f || pw_f) \oplus h(x_a || T_f)$ , where  $ID_f$  is a fake ID of adversary,  $pw_f$  is a randomly chosen fake password, and  $T_f$  is the current timestamp of adversary's machine.
- (ii) Adversary computes  $A_f = h(DID_f || S_n || x_a || T_f)$ , where  $S_n$  is the nearest sensor node for querying the data.
- (iii) Now, adversary sends the message  $\langle DID_f, A_f, T_f \rangle$  to  $S_n$  over insecure communication channel.
- (iv) After receiving the message,  $S_n$  first validates  $T_f$ . If  $(T^* - T_f) \leq \Delta T$ , then  $S_n$  proceeds to next step, otherwise terminates the operation. Here,  $\Delta T$  shows the expected time interval for the transmission delay.
- (v)  $S_n$  now computes  $A'_f = h(DID_f || S_n || x_a || T_f)$  and checks whether the value of  $A'_f \stackrel{?}{=} A_f$  or not. If it holds,  $S_n$  responds to the adversary's query, and  $U_a$ , who is an adversary and not a legitimate user of the sensor network system, enjoys the resources as an authorized user without being a member of the system.

#### 3.2. No Mutual Authentication between GW and Sensor Nodes

In the M.L. Das-scheme, after accepting the login request of  $U_i$ , the GW-node sends a message  $\langle DID_i, A_i, T' \rangle$  to some nearest sensor node  $S_n$ . Here the value of  $A_i$  is computed by  $A_i = h(DID_i || S_n || x_a || T')$ , where  $T'$  is the current timestamp of GW-node. This message informs the sensor node to respond the query/data, which  $U_i$  is requesting from the sensor network. In this message, the value of  $A_i$  is used to ensure the sensor node that it is come from the real GW-node. However, sensor node verifies the authenticity of GW-node but there is no authenticity that the sensor node is fake or real. Thus, the M.L. Das-scheme only provides unilateral authentication between the GW-node and sensor node, and there is not mutual authentication between the two nodes, which is an indispensable property of authentication protocol designing [14].

### 3.3. Privileged-Insider Attack

In a real environment, it is a common practice that many users use same passwords to access different applications or servers for their convenience of remembering long passwords and ease-of-use whenever required. However, if the system manager or a privileged-insider of the GW-node knows the passwords of  $U_i$ , he may try to impersonate  $U_i$  by accessing other servers where  $U_i$  could be a registered user. In the M.L. Das-scheme,  $U_i$  performs registration with GW-node by presenting his password in plain format *i.e.*,  $pw_i$ . Thus, his scheme has pitfalls in terms of insider's attack of GW-node by a privileged user who has come to know the password of  $U_i$  and can misuse the system in future [15].

### 3.4. No Provision for Changing/Updating Passwords

In the M.L. Das-scheme, there is no provision for  $U_i$  to change or update his password whenever required. It is widely recommended security policy for highly secure applications that user's should update or change their passwords frequently, while there is no such option in the M.L. Das-scheme.

## 4. Proposed Security Improvements and Analysis

In this section, we propose security improvements over the scheme of M.L. Das and perform analysis of our security patches as follows:

### 4.1. Introducing Password Change Phase

In this subsection, we introduce the password-change/update phase in the M.L. Das-scheme. In the password-change phase, when a user wants to change his password  $pw_i$  to a new password  $pw_i^*$ , he inserts his smart card into the terminal and enters his ID and password. Smart card validates his  $ID_i$  and  $pw_i$  with the stored values and if the entered  $ID_i$  and  $pw_i$  are correct, then the smart performs the following operations without interacting with GW-node:

- (i) Computes  $N_i^* = N_i \oplus h(ID_i||pw_i) \oplus h(ID_i||pw_i^*)$ , where the value of  $N_i$  is already stored on smart card *i.e.*  $N_i = h(ID_i||pw_i) \oplus h(K)$
- (ii) Smart card replaces the old value of  $N_i$  with the new values  $N_i^*$  and  $h(pw_i^*)$ . Now, the new password is successfully changed and this phase is terminated.

### 4.2. Protection against Insider Attack

As we have mentioned in subsection 3.3, the M.L. Das-scheme has vulnerability of privileged-insider attack due to the reason of presenting his plain text password  $pw_i$  to the GW-node. This problem can simply be overcome if  $U_i$  only submits  $h(pw_i)$  to the GW-node, which is the hashed value of plain text password. Thus in the registration phase, the GW-node would compute  $N_i = h(ID_i||h(pw_i)) \oplus h(K)$ , instead of just  $N_i = h(ID_i||pw_i) \oplus h(K)$ , and the person except  $U_i$  will never know his secret password, which can protect from the possibility of privileged-insider attack [16].

### 4.3. Overcoming GW-node Bypassing Attack and Providing Mutual Authentication

It was identified in subsection 3.1 that there is the possibility of GW-node bypassing attack in M.L. Das-scheme and an adversary without passing the login from the GW-node can access the resources of the sensor network. The reason for the possibility of GW-node bypassing attack is due to sharing of secret parameter  $x_a$  with the sensor node  $S_n$  and user  $U_i$ . If the value of  $x_a$  is compromised, then the whole sensor network will become vulnerable to the GW-node bypassing attack.

Thus, we propose not to share the same secret parameters with  $S_n$  and  $U_i$ , and that every entity has its own secret parameter or key. Here, we suggest that the GW-node should only share  $x_a$  with  $U_i$  and there should be another secret parameter  $x_s$ , which should only be known to the GW-node and sensor nodes, and can be stored in sensor nodes before their deployment in the field. These sensor nodes are responsible to respond users for their queries.

To overcome this security flaw, the Step-V4 and Step-V5 in the verification phase of the M.L. Das-scheme can be amended by the following steps:

- (i) After accepting the login request of  $U_i$ , the GW-node sends message  $\langle DID_i, A_i, T' \rangle$ , to some nearest sensor node  $S_n$  to respond the query/data of  $U_i$ , where  $A_i$  is computed by  $A_i = h(DID_i || S_n || x_s || T')$ . Here  $x_s$  is the secret parameter, which is securely stored in sensor node  $S_n$  and shared only with the GW-node, and  $T'$  is the current timestamp of GW-node's system.
- (ii) Upon receiving the message  $\langle DID_i, A_i, T' \rangle$ , the designated sensor node validates the timestamp. If  $(T'' - T') \leq \Delta T$ , then  $S_n$  proceeds to next step, otherwise terminates the further operation. Here,  $\Delta T$  shows the expected time interval for the transmission delay and  $T''$  is the current timestamp of sensor node  $S_n$ .
- (iii)  $S_n$  now computes  $A_i^* = h(DID_i || S_n || x_s || T')$  and checks whether  $A_i^* \stackrel{?}{=} A_i$  or not. If it holds, then  $S_n$  responds to  $U_i$ 's query, otherwise terminates the operation.
- (iv) To provide mutual authentication between GW-node and sensor node,  $S_n$  now computes  $B_i = h(S_n || x_s || T''')$ . Here  $T'''$  is the current timestamp of sensor node's system and sends back mutual authentication message  $\langle B_i, T''' \rangle$  to the GW-node.
- (v) After receiving the mutual authentication message  $\langle B_i, T''' \rangle$ , the GW-node first checks the validity of time-stamp. If  $(T'''' - T''') \leq \Delta T$ , then GW node performs the further operations, otherwise the mutual authentication phase is terminated. Here,  $\Delta T$  shows the expected time interval for the transmission delay and  $T''''$  is the current timestamp of GW-node.
- (vi) GW-node now computes  $B_i^* = h(S_n || x_s || T''')$  and checks whether  $B_i^* \stackrel{?}{=} B_i$  or not. If it is true, then GW-node establishes trust on sensor node, otherwise, GW-node intimates  $U_i$  about the possibility of malicious sensor node in the network and sends a process-termination message.
- (vii) After successful authentication,  $U_i$  enjoys the resources provided by the sensor network.

Although, in the proposed security patch, the introduction of one more secret parameter  $x_s$  creates storage overhead on the GW-node, but its benefits are two-fold and cannot be overlooked. The first benefit, as defined previously, is to overcome the GW-node bypassing attack, while the second benefit is the ease of secret parameter (key) updating incase of compromise of  $x_s$  by an adversary. In the M.L. Das- scheme, if  $x_a$  is compromised and GW-node has to revoke  $x_a$  with a new secret parameter  $x'_a$ , then

the cost of revoking  $x'_a$  is very high because it needs to be updated on all  $U_i$ 's smart cards as well as all the sensor nodes in the field. While on the other hand, in our proposed security improvement/patch, the cost of revoking secret parameters either  $x_a$  or  $x_s$  can be halved due to assigning different values  $x_a$  and  $x_s$  to  $U_i$  and  $S_n$ , respectively.

## 5. Performance Analysis of Proposed Scheme

In this section, we summarize security features and performance analysis of our proposed scheme and compare its security and robustness with the schemes of M.L. Das [11], and Nyang and Lee [17]. Table 1 demonstrates that our scheme is more secure and robust than the schemes of [11] and [17], and achieves more security features, which were not considered in the aforementioned schemes and are essentially required to implement a practical and universal two-factor user authentication protocol in WSNs.

**Table 1.** Performance analysis and comparison of the proposed scheme.

Security Features and Performance	Proposed scheme	M.L. Das [11]	Nyang-Lee [17]
Securely change/update password	Yes	No	No
Protection against insider's attack	Yes	No	No
Protection against Gateway node bypassing attack	Yes	No	No
Mutual authentication between GW and sensor nodes	Yes	No	Yes
Computational operations in registration phase	3H	2H	2H
Computational operations in login phase	3H	3H	3H
Computational operations in verification phase	7H	5H	12H

H: The computational cost of one hash operation

Furthermore, it can be seen from Table 1 that our scheme needs only 13 hashing operations, in contrast to the protocols of M.L. Das and Nyang-Lee, which require 10 and 17 hash computations, respectively. Our scheme provides protection against insider attack, gateway node bypassing attack, password change/update option, and achieves mutual authentication between gateway and sensor nodes, which require few more hashing operations than [11] to enhance the security of overall authentication system. Hence, the computational overhead of the proposed scheme are not too high, but the scheme contains several enhanced security features, which are indispensable for implementing a reliable and trustworthy remote user authentication scheme in the WSN environment.

## 6. Conclusions

In this paper, we have shown that a recently proposed two-factor user authentication scheme in WSN environment is insecure against different kinds of attack and should not be implemented in real-applications. We have demonstrated that in the M.L. Das-scheme, there is no provision for users to change or update their passwords, the GW-node bypassing attack is possible, it does not provide mutual authentication between GW-node and sensor node, and it is susceptible to privileged-insider attack. To remedy the aforementioned flaws, we have proposed security patches and improvements, which overcome the weak features of the M.L. Das-scheme. The presented security improvements can

easily be incorporated in the M.L. Das-scheme for a more secure and robust two-factor user authentication in WSNs.

## References and Notes

1. Chiara, B.; Andrea, C.; Davide, D.; Roberto, V. An Overview on Wireless Sensor Networks Technology and Evolution. *Sensors* **2009**, *9*, 6869-6896.
2. Callaway, E.H. *Wireless Sensor Networks, Architectures and Protocols*; Auerbach Publications, Taylor & Francis Group: Boca Raton, FL, USA, 2003.
3. Chong, C.Y.; Kumar, S. Sensor Networks: Evolution, Opportunities, and Challenges. *Proc. IEEE* **2003**, *91*, 1247-1256.
4. Benenson, Z.; Felix, C.G.; Dogan, K. User Authentication in Sensor Networks. In *Proceedings of Workshop Sensor Networks*, Ulm, Germany, 2004; pp. 385-389.
5. Watro, R.; Derrick, K.; Sue-fen, C.; Charles, G.; Charles, L.; Peter, K. TinyPK: Securing Sensor Networks with Public Key Technology. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, Washington, DC, USA, 2004; pp. 59-64.
6. Wong, K.H.M; Yuan, Z.; Jiannong, C.; Shengwei, W. A dynamic user authentication scheme for wireless sensor networks. In *Proceedings of Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, Taiwan, 2006; pp. 244-251.
7. Tseng, H.R.; Jan, R.H.; Yang, W. An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks. In *Proceedings of IEEE Globecom*, Washington, DC, USA, 2007; pp. 986-990.
8. Tsern, H.L. Simple Dynamic User Authentication Protocols for Wireless Sensor Networks, In *Proceedings of 2nd International Conference on Sensor Technologies and Applications*, Cap Esterel, France, 2008; pp. 657-660.
9. Ko, L.C. A Novel Dynamic User Authentication Scheme for Wireless Sensor Networks. In *Proceedings of IEEE ISWCS*, Reykjavik, Iceland, 2008; pp. 608-612.
10. Binod, V.; Jorge, S.S.; Joel, J.P.C.R. Robust Dynamic User Authentication Scheme for Wireless Sensor Networks. In *Proceedings of ACM Q2SWinet*, Canary Islands, Spain, 2009; pp. 88-91.
11. Das, M.L. Two-Factor User Authentication in Wireless Sensor Networks. *IEEE Trans. Wireless Comm.* **2009**, *8*, 1086-1090.
12. Kocher, P.; Jaffe, J.; Jun, B. Differential Power Analysis. In *Proceedings of 19<sup>th</sup> International Advances in Cryptology Conference CRYPTO*, Santa Barbara, CA, USA, 1999; pp. 388-397.
13. Messerges, T.S.; Dabbish, E.A.; Sloan, R.H. Examining Smartcard Security under the Threat of Power Analysis Attacks. *IEEE Trans. Comp.* **2002**, *51*, 541-552.
14. Khan, M.K.; Zhang, J. Improving the Security of 'A Flexible Biometrics Remote User Authentication Scheme'. *Comp. Stand. Interf. Elsevier Sci.* **2007**, *29*, 82-85.
15. Ku, W.C.; Chen, S.M. Weaknesses and Improvements of An Efficient Password based Remote user Authentication Scheme using Smart Cards. *IEEE Trans. Cons. Elec.* **2004**, *50*, 204-207.
16. Wang, X.; Zhang W.; Zhang, J.; Khan M.K., Cryptanalysis and Improvement on Two Efficient Remote User Authentication Scheme using Smart Cards. *Comp. Stand. Intefr. Elsevier Sci.* 2007, *29*, 507-512.

17. Nyang, D.H.; Lee M.K. Improvement of Das's Two-Factor Authentication Protocol in Wireless Sensor Networks, *Cryptology* ePrint Archive 2009/631. Online PDF: <http://eprint.iacr.org/2009/631.pdf> (accessed on 28 February 2010).

© 2010 by the authors; licensee Molecular Diversity Preservation International, Basel, Switzerland. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/>).