# On the Security of 'An Efficient Biometric Authentication Protocol for Wireless Sensor Networks'

Ashok Kumar Das

Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad 500 032, India
iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in

**Abstract.** In 2013, Althobaiti et al. proposed an efficient biometric-based user authentication scheme for wireless sensor networks. We analyze their scheme for the security against known attacks. Though their scheme is efficient in computation, in this paper we show that their scheme has some security pitfalls such as (1) it is not resilient against node capture attack, (2) it is insecure against impersonation attack and (3) it is insecure against man-in-the-middle attack. Finally, we give some pointers for improving their scheme so that the designed scheme needs to be secure against various known attacks.

**Keywords:** Wireless sensor networks, User authentication, Smart cards, Biometrics, Cryptanalysis.

## 1 Introduction

A wireless sensor network (WSN) is considered as a large network having several tiny computing nodes, also called the sensors or motes. These nodes are deployed in a deployment field or target field. These nodes have the ability to sense important observations from their surrounding areas and the transmit those sensing data to the nearby *base stations*, which do further processing on behalf of them. Sensor nodes can communicate among each other by short range radio communications. The base station is considered a most powerful node in WSN. On the other hand, the sensor nodes are extremely resource-starved, which lack of memory, computational capability as well as radio transmission range.

Sensor networks are widely used in a variety of applications ranging from military to environmental and medical research in recent years. In many applications including target tracking, battlefield surveillance and intruder detection, WSNs often operate in hostile and unattended public environments. Thus, an adversary has an opportunity to directly capture a sensor node directly from the target field and extract all the information from its memory as the sensor nodes are generally not equipped with the tamper-resistant devices due to their cost constraints. Hence, there is a strong need for protecting the sensing data and sensing readings in WSNs. In wireless environments, an adversary not only can eavesdrop the radio traffic, but also has the ability to intercept or interrupt the exchanged messages. As a result, several protocols and algorithms designed for the traditional networks do not work in hostile environments unless we take care of the adequate security measures. Hence, security in WSNs becomes an important concern as there are several potential attacks against sensor networks. The readers can find a survey on wireless sensor networks and their security issues in [1], [3], [4], [6], [18].

We consider the necessity of a user authentication problem in WSNs as follows. Several critical applications in WSNs are real-time based and the users (called the external parties) usually want to access the real-time data from the nodes inside WSNs [9]. Such an access in WSNs is possible, if we allow the users to access the real-time data directly from the nodes and not from the base station, because the data available at the base station may not be always real-time and they are gathered periodically by the base station from the nodes in WSNs. To access the real-time data from the nodes, the user needs to be first authenticated to the nodes as well as the base station and then need to establish a secret session key between the user and the accessed node so that the illegal access to nodes do not happen by an adversary. Due to this reason, the user authentication problem is a very important research topic in WSN security, which has received considerable research attention in WSN security study in the recent years.

Several password-based user authentication schemes have been proposed in the literature [5], [12], [13], [14], [16], [20], [22]. However, most of these schemes are insecure against various known attacks. Das et al. [9] proposed a novel and efficient password-based user authentication scheme for the hierarchical wireless sensor networks. Their scheme was shown to be secure against various known attacks including the replay and man-in-the-middle attacks with the help of formal security verification [7]. Further, an improved version of Das et al.'s scheme [9] has been proposed in [21] in the literature. Recently, biometric-based user authentication in WSNs has drawn a considerable research attention. Thus, the biometric-based user authentication in WSN becomes inherently more reliable and secure than usual traditional password-based user authentication schemes. Yuan et al.'s biometric-based user authentication scheme [23] provides better security as compared to that for M. L. Das's scheme [10] because the former scheme uses biometrics verification along with the password verification of the user. Yuan et al.'s scheme [23] has same drawbacks as in M. L. Das's scheme [10]. However, their scheme cannot resist denial-of-service attack and node compromise attack. Das et al. proposed a new secure biometric-based user authentication scheme in hierarchical wireless body area sensor networks [8]. Althobaiti et al. [2] proposed an efficient biometric-based user authentication scheme for WSNs. Unfortunately, we show that their scheme has several security pitfalls and as a result, their scheme is not practical to use for the real-life WSN applications.

The roadmap of this paper is sketched as follows. In Section 2, we describe the Althobaiti et al.'s scheme [2]. We then show that Althobaiti et al.'s scheme is insecure against four attacks in Section 3. In Section 4, we point out some suggestions to improve Althobaiti et al.'s scheme in order to withstand those security pitfalls. Finally, we conclude the paper in Section 5.

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

In this section, we briefly review the recently proposed Althobaiti et al.'s biometric based user authentication scheme in wireless sensor networks [2]. The different phases of their scheme are discussed in the following subsections. We use the notations listed in Table 1 for describing and analyzing Althobaiti et al.'s scheme.

**Table 1.** The notations used in this paper

| Symbol | Explanation |
|---|---|
| $U_i$ | $i^{th}$ user |
| $SN_j$ | Identity of the $j^{th}$ sensor node $SN_j$ |
| $X$ | Secret information shared by GW-node and all deployed sensor nodes |
| $E_k(\cdot)$ | Symmetric encryption using the key $k$ |
| $D_k(\cdot)$ | Symmetric decryption using the key $k$ |
| $MAC_k(m)$ | Message authentication code of $m$ using the key $k$ |
| $h(\cdot)$ | Secure one-way collision-resistant hash function |
| $A\|\|B$ | Data $A$ concatenates with data $B$ |
| $A \oplus B$ | Data $A$ is bitwise XORed with data $B$ |

### 2.1 Registration Phase

For the registration of a user $U_i$, the system randomly selects an encryption key, say $ek_i$, and it is saved in the GW-node or the base station (BS) as a key of $U_i$. The features of $U_i$'s biometric (for example, iris) are extracted and then hashed by the one-way hash function $h(\cdot)$ (for example, SHA256 [19]). After that the hash digest is XORed with the key $ek_i$ in order to generate BE template, which is then saved in $U_i$'s device. In this phase, the user $U_i$'s data (identity $ID_i$, name, etc.) and $ek_i$ are saved in the GW-node's database. The GW-node computes $F_i = h(ID_i \oplus X)$, where $X$ is a secret parameter generated by the GW-node and it is also saved in all the sensor nodes $SN_j$ (the sensor login-nodes) before the deployment of those sensor nodes in a particular target field. Finally, the GW-node sends the registration message $\langle ID_i, F_i \rangle$ to the user $U_i$ via a secure channel. In this scheme, as in M. L. Das's scheme [10], all the deployed sensor nodes $SN_j$ are responsible to respond to the data/query that the users $U_i$ are looking for and know the secret parameter $X$. Note that $U_i$'s device contains the information $\{ID_i, F_i, h(ek_i), BE\}$, where $BE = h(biometric\_feature) \oplus ek_i$.

### 2.2 Login Phase

In this phase, the following steps are executed:

Step 1. A legal user $U_i$ first inputs his/her identity $ID_i$ and then the personal biometric, iris by camera in the device. The biometric features of $U_i$'s iris are then extracted, corrected by error correcting code, and also hashed by SHA256 hashing algorithm.

Step 2. The hashed value is bitwise XORed with the saved BE template in $U_i$'s device in order to regenerate the encryption key $ek_i' = BE \oplus h(biometric\_feature)$.

Step 3. $ek_i'$ is hashed and after that $h(ek_i)$ stored in the device is compared with the computed $h(ek_i')$. If there is a match, a login request $\langle ID_i, request\rangle$ is sent to the GW-node along with $ID_i$ via a public channel. Otherwise, the session is terminated immediately.

### 2.3 Authentication Phase

This phase has the following steps:

Step 1. After receiving the login request from $U_i$, the GW-node replies to the user $U_i$ with the authentication request $\langle R\rangle$, where $R$ is a random challenge. When $U_i$ receives the message from the GW-node, $U_i$ encrypts $R$ and $T_1$ with the encryption key $ek_i$ derived in the login phase, where $T_1$ is the current timestamp of $U_i$'s device, and sends the authentication request message $\langle E_{ek_i}(R, T_1)\rangle$ to the GW-node via a public channel.

Step 2. After receiving the authentication request message from the user $U_i$, the GW-node decrypts the message using the encryption key $ek_i$ stored in the GW-node and checks the condition $|T_1 - T_2| < \Delta T$, where $\Delta T$ denotes the interval of the expected time for the transmission delay in WSN and $T_2$ the time when the message was received. If this condition is invalid, the authentication phase is terminated immediately.
The GW-node computes $F_i = h(ID_i \oplus X)$ and $Y_i = MAC_{F_i}(ID_i||SN_j||T_3)$, where $SN_j$ denotes the sensor node which is supposed to reply to the query made by the user $U_i$, and $T_3$ is the GW-node's current timestamp. The GW-node then sends the message $\langle ID_i, Y_i, T_3\rangle$ to $SN_j$ via a public channel.

Step 3. When $SN_j$ receives the message from the GW-node, $SN_j$ checks the validity of $T_3$ by verifying the condition $|T_3 - T_4| < \Delta T$, where $T_4$ is the time when the message was received. If the condition is valid, $SN_j$ computes $F_i = h(ID_i \oplus X)$, $Y_i' = MAC_{F_i}(ID_i||SN_j||T_3)$ and checks if $Y_i' = Y_i$. If it holds, $SN_j$ responds to the $U_i$'s query (RM), computes $V_i = h(ID_i||F_i||T_5)$, $C_i = h(RM)$ and $L = E_{V_i}(RM, C_i)$, and then sends the message $\langle L, T_5\rangle$ to the user $U_i$ via a public channel, where $T_5$ is the $SN_j$'s current timestamp.

Step 4. Finally, when the user $U_i$ receives the message from $SN_j$ at time $T_6$, $U_i$ first validates by checking whether $|T_5 - T_6| < \Delta T$, and if it is valid then $U_i$ computes $V_i = h(ID_i||F_i||T_5)$. After that $U_i$ decrypts $L$ to retrieve $RM$ and $C_i$ as $(RM', C_i') = D_{V_i}(L)$, and then computes $C_i^* = h(RM')$. If $C_i^* = C_i'$, $U_i$ accepts $RM$ as a valid query response from $SN_j$. Otherwise, $U_i$ rejects

$RM$. Note that in this scheme $V_i = h(ID_i||F_i||T_5)$ is considered as a session key between $U_i$ and $SN_j$.

**Table 2.** Summary of exchanged messages in the login and authentication phases

| User $U_i$ | GW-node | Sensor $SN_j$ |
|---|---|---|
| *Login phase* | | |
| $\xrightarrow{\langle ID_i, request \rangle}$ | | |
| *Authentication phase* | | |
| | $\xleftarrow{\langle \text{A random challenge, } R \rangle}$ | |
| $\xrightarrow{\langle E_{ek_i}(R, T_1) \rangle}$ | | |
| | $\xrightarrow{\langle ID_i, Y_i, T_3 \rangle}$ | |
| Receives $\langle L, T_5 \rangle$ from $SN_j$ | | $\xleftarrow{\langle L, T_5 \rangle}$ |

The summary of the login phase and authentication phase of Althobaiti et al.'s scheme is provided in Table 2.

## 3 Cryptanalysis of Althobaiti et al.'s Scheme

In this section, we first supply a threat model in Section 3.1 under which the security of WSN is generally evaluated. After that we show that Althobaiti et al.'s scheme is insecure against several attacks, which are outlined in Section 3.2.

### 3.1 Threat Model

For evaluating the security analysis of Althobaiti et al.'s scheme, we use the threat model as follows. In most applications, sensor are usually deployed in the hostile environments. We assume that due to cost constrains, the deployed sensor nodes are not equipped with tamper-resistant devices. Further, we assume that sensor nodes can be physically captured by an adversary either randomly or selectively from the target field. Once a node is captured by an adversary, all the sensitive data as well as cryptographic secret data stored in its memory are known to that adversary. From the literature it is known that even if the sensor nodes are equipped with the tamper-resistant devices, an adversary can still extract all the sensitive data stored in their memory by monitoring the power analysis attacks [15], [17]. However, in any case, the base station or gateway node (GW) will not be compromised by an adversary, because if the base station is compromised, the entire network may be compromised. As in [10], the Dolev-Yao threat model [11] is used in this paper, in which two nodes communicate over a public channel. This threat model is suitable for WSNs, because the channel is insecure and the end-points (sensor nodes) cannot in general be trusted. An adversary has the ability to eavesdrop on all traffic, inject packets and reply the old previous messages during the transmissions.

### 3.2 Attacks on Althobaiti et al.'s Scheme

In this section, we show that Althobaiti et al.'s scheme is insecure against the following attacks.

**Resilience against node capture attack** The definition of the resilience against node capture attack of a user authentication scheme in WSN is taken from [9] as follows. Suppose $c$ nodes are captured either randomly or selectively in the target field by an adversary. Then the adversary knows all the information from their memory. Knowing these infromation, the adversary cam compromise a fraction of total secure communications that are compromised by $c$ nodes *not including* the communication in which those nodes are directly involved. Thus, this reflects on the effect of $c$ sensor nodes being compromised on the rest of the network. Let $P_e(c)$ denote the probability that the adversary can decrypt the secure communication between a non-compromised sensor node $SN_j$ and a user $U_i$ when $c$ nodes are already comprmised. If $P_e(c) = 0$, a user authentication scheme is called *unconditionally secure against node capture attack*.

Suppose an adversary (attacker) captures a login-sensor node, say $SN_j$. Then the adversary knows the secret parameter $X$ stored in the sensor $SN_j$'s memory and the GW-node. Intercepting the messages $\langle ID_i, Y_i, T_3\rangle$ and $\langle L, T_5\rangle$ during the authentication phase, the adversary can compute $F_i = h(ID_i \oplus X)$ and $V_i = h(ID_i||F_i||T_5)$, which is the session key between a user $U_i$ and the sensor $SN_j$. Hence, the adversary knows the session key $V_i$. We now show that the adversary has the ability to compromise all the session keys between $U_i$ and any other non-compromised sensor node $SN_j'$ as follows. Let the GW-node send the message $\langle ID_i, Y_i', T_3'\rangle$ to $SN_j'$ and the sensor $SN_j'$, which is a non-compromised node, send the message $\langle L', T_5'\rangle$ during the authentication phase, where $F_i = h(ID_i \oplus X)$, $Y_i' = MAC_{F_i}(ID_i||SN_j'||T_3')$, $C_i' = h(RM)$, $V_i' = h(ID_i||F_i||T_5')$ and $L' = E_{V_i'}(RM, C_i')$. Since the adversary knows $X$, $ID_i$ and $T_5'$, so he/she can easily derive the session key $V_i' = h(ID_i||F_i||T_5')$. It is then clear that the adversary can derive all the session keys between $U_i$ and any non-compromised sensor node $SN_j'$ even if a single login-sensor node is already compromised in WSN. As a result, compromise of a single sensor node leads to compromise the successful decryptions of all secure communications between $U_i$ and any non-compromised sensor $SN_j'$. Thus, we have $P_e(c) = 1.0$. Hence, Althobaiti et al.'s scheme is not at all resilient against node capture attack.

**Impersonation attack** In this attack, we show that an adversary $\mathcal{A}$ can impersonate the GW-node to a login sensor node. The detailed description is as follows. Suppose $\mathcal{A}$ physically captures a login-sensor node, say $SN_j$. $\mathcal{A}$ then knows the secret parameter $X$ from the captured node $SN_j$. $\mathcal{A}$ also intercepts the message $\langle ID_i, Y_i, T_3 \rangle$ during the authentication phase. Let $\mathcal{A}$ wish to impersonate the GW-node to another non-compromised login-sensor node $SN'_j$. For this purpose, $\mathcal{A}$ can compute $F'_i = h(ID_i \oplus X)$ and $Y'_i = MAC_{F'_i}(ID_i||SN'_j||T'_3)$, where $SN'_j$ denotes the sensor node from which the user $U_i$ is expecting the response of the query, and $T'_3$ is the current timestamp of the adversary $\mathcal{A}$'s system. $\mathcal{A}$ then sends the message $\langle ID_i, Y'_i, T'_3 \rangle$ to $SN'_j$ via a public channel. After receiving the message, $SN'_j$ checks checks the validity of $T'_3$. If it is valid, $SN'_j$ computes $F_i = h(ID_i \oplus X)$, $Y^*_i = MAC_{F_i}(ID_i||SN'_j||T'_3)$ and checks the condition $Y^*_i = Y'_i$. If it holds, $SN'_j$ responds to the user $U_i$'s query ($RM'$), computes the session key $V'_i = h(ID_i||F_i||T'_5)$, $C'_i = h(RM')$ and $L' = E_{V'_i}(RM', C'_i)$, where $T'_5$ is the current timestamp of $SN'_j$, and finally sends the message $\langle L', T'_5 \rangle$ to $U_i$ via a public channel. Note that in this case, $\mathcal{A}$ can also derive the session key $V'_i$ using $X$, $ID_i$ and $T'_5$. As a result, Althobaiti et al.'s scheme fails to protect the impersonation attacks.

**Man-in-the-middle attack** In this attack, an adversary $\mathcal{A}$ tries to modify, delete or change the contents of the messages in such a way that the login-sensor nodes as well as the user $U_i$ can not detect them. Assume that $\mathcal{A}$ captures a login-sensor node and then he/she knows the secret parameter $X$ from its memory. Suppose the GW-node sends the message $\langle ID_i, Y_i, T_3 \rangle$ to a login-sensor node $SN_j$ from which the user $U_i$ wants to get the response of the query. The adversary $\mathcal{A}$ intercepts this message, computes $F^*_i = h(ID_i \oplus X)$ using $ID_i$ and extracted $X$, $Y^*_i = MAC_{F^*_i}(ID_i||SN_j||T^*_3)$, where $T^*_3$ is the current timestamp of the adversary $\mathcal{A}$'s system, and sends the modified message $\langle ID_i, Y^*_i, T^*_3 \rangle$ to the sensor node $SN_j$ instead of the original message $\langle ID_i, Y_i, T_3 \rangle$ via a public channel.

After receiving the message from $\mathcal{A}$, $SN_j$ believes that the message comes from the GW-node and proceeds to validate the timestamp $T^*_3$ and if it is valid, $SN_j$ computes $F_i = h(ID_i \oplus X)$, $Y^{**}_i = MAC_{F_i}(ID_i||SN_j||T^*_3)$ and checks the condition $Y^{**}_i = Y^*_i$. If it holds, $SN_j$ responds to the $U_i$'s query ($RM^*$) by computing the session key shared with the user $U_i$ as $V^*_i = h(ID_i||F_i||T^*_5)$, $C^*_i = h(RM^*)$ and $L^* = E_{V^*_i}(RM^*, C^*_i)$, and then sending the message $\langle L^*, T^*_5 \rangle$, where $T^*_5$ is the current timestamp of $U_i$'s device. $\mathcal{A}$ again intercepts the message $\langle L^*, T^*_5 \rangle$. $\mathcal{A}$ computes $V^{**}_i = h(ID_i||F^*_i||T^*_5)$ and decrypts $L^*$ to retrieve $RM^*$ and $C^*_i$. Note that $\mathcal{A}$ now knows the response to the query, $RM^*$ which is intended for $U_i$ only. However, $\mathcal{A}$ can create a totally face response $RM^{**}$ to the query instead of the original $RM^*$, and compute $C^{**}_i = h(RM^{**})$ and $L^{**} = E_{V^{**}_i}(RM^{**}, C^{**}_i)$. Finally, $\mathcal{A}$ can send the modified message $\langle L^{**}, T^*_5 \rangle$ to the user $U_i$. It is noted that this message is successfully authenticated by the user $U_i$, and hence $U_i$ treats $RM^{**}$ as a valid response to his/her query. Thus, it is clear that Althobaiti et al.'s scheme fails to protect the man-in-the-middle attack.

## 4 Discussions

From the cryptanalysis of Althobaiti et al.'s scheme discussed in Section 3.2, it is clear that their scheme becomes insecure due to the fact that the master secret parameter $X$ is stored in every deployed sensor node, which is also shared with the GW-node as in M. L. Das's scheme [10]. As a remedy, one solution could be to generate a unique random master key $MK_{SN_j}$ for each sensor node $SN_j$ in WSN by the GW-node in offline, and then only $MK_{SN_j}$ needs to be preloaded in the sensor node $SN_j$'s memory prior to its deployment in the target field and also in the GW-node as pointed out in Das et al.'s scheme [9]. This strategy will certainly help to improve significantly the resilience against node capture attack, because compromise of a sensor node only reveals its master key, not the master keys of any other non-compromised sensor nodes. As a consequence, other attacks will also be eliminated. In future, we aim to propose an improvement on Althobaiti et al.'s scheme in order to withstand the security weaknesses found in their scheme.

## 5 Conclusion

In this paper, we have first reviewed the recently proposed Althobaiti et al.'s scheme suited for WSNs. Althobaiti et al.'s scheme is efficient in computation. Unfortunately, we have shown that their scheme is insecure against several known attacks. Thus, their scheme is not suitable for practical application in WSNs. In addition, we have suggested some strategies in order to remedy the security weaknesses found in their scheme.

## References


1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A Survey. *Computer Networks*, 38(4):393–422, 2002.
2. O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan. An efficient biometric authentication protocol for wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2013:1–13, 2013. Article ID 407971, http://dx.doi.org/10.1155/2013/407971.
3. S. Chatterjee, A. K. Das, and J. K. Sing. Analysis and Formal Security Verification of Access Control Schemes in Wireless Sensor Networks: A Critical Survey. *Journal of Information Assurance and Security*, 8(1):33–57, 2013.
4. S. Chatterjee, A. K. Das, and J. K. Sing. A survey on user access control in wireless sensor networks with formal security verification. *International Journal of Trust Management in Computing and Communications*, 2014. In Press.
5. T.-H. Chen and W.-K. Shih. A Robust Mutual Authentication Protocol for Wireless Sensor Networks. *ETRI Journal*, 32(5):704–712, Oct. 2010.
6. A. K. Das. A Survey on Analytic Studies of Key Distribution Mechanisms in Wireless Sensor Networks. *Journal of Information Assurance and Security*, 5(5):526–553, 2010.

7. A. K. Das, S. Chatterjee, and J. K. Sing. Formal Security Verification of a Dynamic Password-Based User Authentication Scheme for Hierarchical Wireless Sensor Networks. In *International Symposium on Security in Computing and Communications (SSCC 2013), Communications in Computer and Information Science Series (CCIS)*, volume 377, pages 243–254, 2013.
8. A. K. Das, S. Chatterjee, and J. K. Sing. A New Biometric-Based Remote User Authentication Scheme in Hierarchical Wireless Body Area Sensor Networks. *Ad Hoc & Sensor Wireless Networks*, 2014. In Press.
9. 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*, 35(5):1646–1656, 2012.
10. M. L. Das. Two-Factor User Authentication in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications*, 8(3):1086–1090, 2009.
11. D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.
12. R. Fan, L.-D. Ping, J.-Q. Fu, and X.-Z. Pan. A Secure and Efficient User Authentication Protocol for Two-Tieres Wireless Sensor Networks. In *Second Pacific-Asia Conference on Circuits, Communications and System (PACCS 2010)*, pages 425–428, 2010.
13. D. He, Y. Gao, S. Chan, C. Chen, and J. Bu. An Enhanced Two-Factor User Authentication Scheme in Wireless Sensor Networks. *Ad Hoc & Sensor Wireless Networks*, 10(4):361–371, 2010.
14. M. K. Khan and K. Alghathbar. Cryptanalysis and Security Improvements of Two-Factor User Authentication in Wireless Sensor Networks. *Sensors*, 10:2450–2459, 2010.
15. P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Proceedings of Advances in Cryptology - CRYPTO'99, LNCS*, volume 1666, pages 388–397, 1999.
16. C.-C. Lee, C.-T. Li, and S.-D. Chen. Two Attacks on a Two-Factor User Authentication in Wireless Sensor Networks. *Parallel Processing Letters*, 21(1):21–26, 2011.
17. 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*, 51(5):541–552, 2002.
18. A. Perrig, J. Stankovic, and D. Wagner. Security in wireless sensor networks. *Communications of the ACM*, 47(6):53–57, 2004.
19. Secure Hash Standard. FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995.
20. B. Vaidya, D. Makrakis, and H. T. Mouftah. Improved Two-Factor User Authentication in Wireless Sensor Networks. In *Second International Workshop on Network Assurance and Security Services in Ubiquitous Environments*, pages 600–606, 2010.
21. D. Wang and P. Wang. Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. *Ad Hoc Networks*, 2014. In Press. http://dx.doi.org/10.1016/j.adhoc.2014.03.003.
22. K. Wong, Y. Zheng, J. Cao, and S. Wang. A dynamic user authentication scheme for wireless sensor networks. In *Proceedings of IEEE International Conf. Sensor Networks, Ubiquitous, Trustworthy Computing, IEEE Computer Society*, pages 244–251, 2006.
23. J. Yuan, C. Jiang, and Z. Jiang. A Biometric-Based User Authentication for Wireless Sensor Networks. *Wuhan University Journal of Natural Sciences*, 15(3):272–276, 2010.