

A Robust Password-based Authentication Scheme for Heterogeneous Sensor Networks

Huei-Ru Tseng, Rong-Hong Jan, and Wu Yang*

Department of Computer Science, National Chiao Tung University

*E-mail: wuyang@cs.nctu.edu.tw

Abstract

User authentication is a critical security function for computer systems that allow legitimate users remote access over an insecure communication network. In this paper, we propose a new password-based authentication scheme for heterogeneous sensor networks that consist of sensor nodes of different types. The proposed scheme allows legitimate users to query sensor data at any sensor node in the network, provides not only mutual authentication but also key agreement between a user and a sensor node, and adopts fuzzy identity-based encryption for gateway nodes and high-end sensor nodes. Additionally, our analysis shows that the proposed scheme is immune to some of the most notorious attacks, such as replay attacks, forgery attacks, offline-dictionary attacks, stolen smart card attacks, insider attacks, and many other potential breaches of security.

1. Introduction

Wireless sensor networks (WSNs) are networks consisting of spatially distributed sensors which cooperatively monitor environmental conditions, such as humidity, pressure, temperature, motion, or vibration, at different locations. The collected data can be presented to users either when polled or upon event detection. In general, most queries in WSN applications are issued at the base stations or at the backend of the application system. However, real-time data may no longer be accessed only at the base stations or the gateway nodes. With the increasing ubiquity of WSNs, any sensor node might be accessed to acquire real-time data.

For some applications, such as military surveillance, the collected data is highly sensitive. Hence, security measures should be taken to protect the collected secrets in order to prevent un-authorized users from gaining the information. Over the last few years, there has been a dramatic increase in the number of publications on user authentication [1-14]. However, to date, most existing research on user authentication [15-20] considers homogeneous sensor networks, which consist of identical sensors with equal capacity in terms of sensing, computation, communication, and power. Several recent works [21-27] have shown that heterogeneous sensor networks (HSNs) can significantly improve network performance.

In this paper, we propose a new robust password-based authentication scheme for HSNs that allows legitimate users to query sensor data at any sensor node in the network. To the best of our knowledge, the proposed scheme is also the first user authentication scheme that adopts *fuzzy identity-based encryption* [28-29] for gateway nodes and high-end sensor nodes in HSNs. We will

discuss this concept in detail later.

Additionally, the proposed scheme provides many desirable features: (1) it does not require a registration gateway node to maintain a password table for verifying the legitimacy of login users; (2) it allows users to choose and change their passwords freely and hence give users more convenience; (3) it achieves mutual authentication and key agreement between users and sensor nodes; (4) it does not require synchronized clocks between users and sensor nodes. Moreover, the proposed scheme can resist many well-known attacks.

The rest of this paper is organized as follows: In Section 2, we briefly review several existing user authentication schemes for homogeneous sensor networks. Next, we introduce our system model in Section 3. Then, in Section 4, we propose a robust password-based authentication scheme for HSNs and analyze the proposed scheme in Section 5. Finally, we conclude our paper in Section 6.

2. Related Works

User authentication in homogeneous sensor networks was first proposed by Benenson et al. [15] in 2004. They investigated several security issues in WSNs, especially the problem of access control, and also introduced the notion of *n-authentication*, which means the authentication succeeds if the user can be successfully authenticated with at least $(n-t)$ of n sensors, where t means the number of sensor nodes that the adversary can compromise. Thereafter, Benenson et al. [16] proposed the first solution to the user authentication problem in the presence of node capture attacks. The scheme is based on public key cryptography and elliptic curve cryptosystem (ECC), and is designed for a sensor node to authenticate the user.

In 2006, Wang and Li [17] proposed a distributed user access control scheme under a realistic adversary model in sensor networks. The scheme is based on ECC. Their user authentication scheme is divided into local authentication conducted by the sensor that is physically close to the user and remote authentication based on the endorsement of the local sensors. Recently, Jiang et al. [18] proposed a distributed user authentication scheme based on the self-certified keys cryptosystem and used ECC to establish pair-wise keys between users and sensor nodes.

However, some weaknesses were pointed out: an adversary might send a bogus certificate and signature in the authentication phase. Thus, there was still possibility of an impersonation attack [19]. Moreover, the computational overhead is very high in the above schemes. In order to achieve better performance, Wong et al. [19] proposed the first password-based user authentication scheme for WSNs. Compared with earlier works, this scheme is extremely efficient in terms of the computational cost since the protocol participants perform only a few hash operations. Unfortunately, Tseng et al. [20] showed that Wong et al.'s scheme suffers from vulnerability to both replay and forgery attacks and proposed an improved scheme to enhance the security of Wong et al.'s scheme.

Previous works on user authentication [15-20] are mainly concerned with homogeneous sensor networks. To achieve better security and efficiency, we propose the robust password-based user authentication scheme for HSNs. To the best of our knowledge, this is the first proposal for user

authentication in HSNs. Our scheme can resist several well-known attacks, such as replay attacks, forgery attacks, offline-dictionary attacks, stolen smart card attacks, insider attacks, and many other potential breaches of security.

3. System Model and Assumptions

A heterogeneous sensor network (HSN) consists of two types of sensors: a small number of powerful high-end sensors (H-sensors) and a large number of low-end sensors (L-sensors). An HSN is divided into multiple clusters, where each H-sensor serves as the cluster head and each L-sensor joins the cluster headed by the closest H-sensor. Details of the clustering schemes can be found in [25-27]. The general model of an HSN [24-27] is described below.

- H-sensors are equipped with tamper-resistant hardware to protect key material preloaded in the registration phase.
- L-sensors are not equipped with tamper-resistant hardware. This implies that if an L-sensor is compromised, its contents will be considered revealed.
- Both L-sensors and H-sensors are aware of their own location.

In HSN, we assume that the sensor gateway (GW) node is responsible for generating the secret parameters for each user and H-sensor. In previous works [19-20], user authentication is done solely by the GW. However, these kinds of centralized authentication schemes might easily suffer from single-point-failure attacks and DoS attacks [18]. In order to conquer such problems, the proposed scheme adopts *fuzzy-identity encryption* [28-29]:

In a fuzzy identity-based encryption scheme, an entity with the secret key for the identity w is able to decrypt a ciphertext encrypted with the public key w' if and only if w and w' are within a certain distance of each other as judged by some metric.

Prior to the deployment, each H-sensor is loaded with a secret key derived from the GW's secret key. The derivation of secret keys can be done with the fuzzy identity-based encryption. Thus, an H-sensor with a secret key w is able to decrypt a ciphertext encrypted with the GW's secret key w' if and only if w and w' are within a certain distance of each other.

As noted in [28-29], there is another application of fuzzy identity-based schemes which is "*attribute-based encryption*" [30-31] where a party can encrypt data to all users that have a certain set of attributes, e.g. {company, division, department}. Therefore, the GW can also dynamically choose the H-sensor with certain set of attributes to decrypt a ciphertext encrypted by the GW. More details of fuzzy identity-based schemes can be found in [28-29]. Therefore, we can distribute the right of authentication into H-sensors against the attacks mentioned above.

4. Proposed Scheme

The proposed scheme is divided into three phases: registration, login-and-authentication, and password-change. Registration and password-change are performed via a secure channel. We list our notations and their corresponding definitions in Table 1.

Table 1 Notations

| Symbol | Definition |
|-------------|---|
| U_i | User i |
| ID_i | User i 's identity |
| PW_i | User i 's password |
| x | The gateway node's secret key |
| n | $n = p \times q$, where $p \equiv q \equiv 3 \pmod{4}$ |
| sk_i | A session key computed by user i and an H-sensor |
| $h(\cdot)$ | A one-way hash function |
| \parallel | Concatenation |

4.1. The Registration Phase

Firstly, the sensor gateway (GW) node randomly chooses a string x as its secret key for symmetric encryption. Next, it randomly selects two distinct large primes (p, q) , where $p \equiv q \equiv 3 \pmod{4}$, and computes $n = p \times q$. Then, each H-sensor preloads (p, q) and keeps them as secrets. The GW uses its secret key x to derive each H-sensor's secret key with fuzzy identity-based encryption.

We assume a registration interface is launched on a user's mobile device, such as a PDA, PC, etc. The mobile device is assumed to have the ability to communicate with the sensor nodes within an HSN. Suppose a new user U_i with the identity ID_i and password PW_i wants to register with the GW for services. The registration procedures are presented as follows.

1. U_i sends $(ID_i, h(PW_i))$ to the GW via a secure channel.
2. Upon receiving the registration message, the GW computes y_i :

$$y_i = E_x(h(x) \parallel ID_i \parallel h(PW_i)) \tag{1}$$

where $E_x(\cdot)$ denotes a symmetric encryption using the secret key x . Then, the GW stores $(ID_i, y_i, h(\cdot), n)$ in a smart card.

3. The GW issues the smart card to U_i via a secure channel, and sends ID_i to each sensor login-node. Upon receiving ID_i , each sensor login-node stores it in its database.

Note that either an L-sensor or an H-sensor could be a sensor login-node. We assume the L-sensor is the login-node in this paper. The overall operations of the registration phase are illustrated in Figure 1.

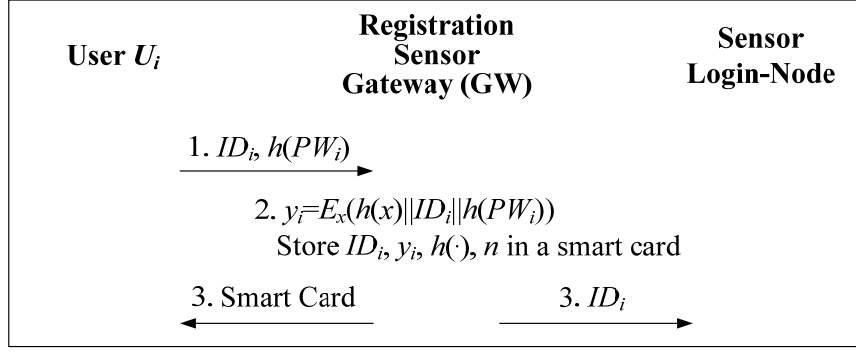


Figure 1. The registration phase of the proposed scheme.

4.2. The Login-and-Authentication Phase

When a user wishes to query sensor data, he/she has to log in to a sensor login-node. U_i first enters his/her identity ID_i and password PW_i^* . The details are presented as follows.

1. U_i computes the pair (w_0, C_0) :

$$w_0 = (ID_i \parallel y_i \parallel u)^2 \bmod n \quad (2)$$

where u is randomly chosen by U_i .

$$C_0 = (ID_i \parallel w_0) \quad (3)$$

2. U_i sends C_0 to the login-node as a login request.
3. After receiving the login information C_0 , the login-node checks whether ID_i exists in the list of datasets.
4. If so, the login-node relays C_0 to the closest H-sensor for authentication. Otherwise, it rejects the login request.
5. Upon receiving the login request, the H-sensor first uses (p, q) to decrypt w_0 and obtain (ID_i, y_i, u) with Rabin's algorithm [32]. It then decrypts y_i via the secret key and obtains $(h(x) \parallel ID_i \parallel h(PW_i))$. Next, it verifies whether $h(x)$ is correct and whether ID_i in y_i equals ID_i in w_0 . If so, it keeps $h(PW_i)$ for later use and computes C_1 :

$$C_1 = E_u(ID_i \parallel h(u) \parallel v) \quad (4)$$

where v is randomly chosen by the H-sensor.

6. The H-sensor sends C_1 to the login-node.
7. The login-node relays C_1 to U_i .

8. U_i decrypts C_1 using u and then obtains $(ID_i || h(u) || v)$. Next, U_i verifies $h(u)$ to ensure that C_1 indeed comes from the H-sensor. Then, U_i computes C_2 :

$$C_2 = E_v(ID_i || h(v) || h(PW_i^*)) \quad (5)$$

9. U_i sends C_2 to the login-node.
 10. The login-node relays C_2 to the H-sensor.
 11. Upon receiving C_2 , the H-sensor decrypts C_2 to ensure C_2 was indeed sent by U_i . Finally, it checks whether $h(PW_i^*) = h(PW_i)$. If so, the H-sensor accepts the login request of U_i and computes sk_i :

$$sk_i = h(h(PW_i) || u || v) \quad (6)$$

The overall operation of the login-and-authentication phase is illustrated in Figure 2.

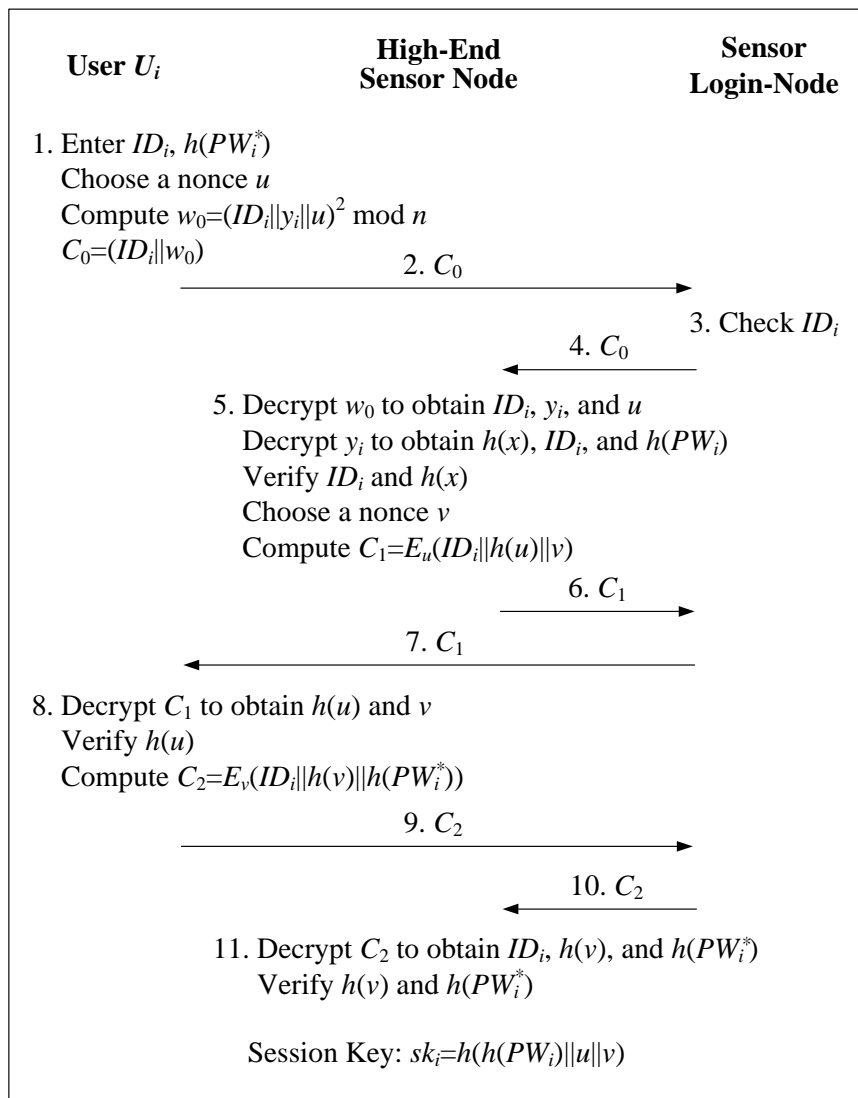


Figure 2. The login-and-authentication phase of the proposed scheme.

4.3. The Password-Change Phase

If the user wants to change his/her password, he/she needs to perform the following operations.

1. U_i first chooses a new password PW_i' and sends his/her identity ID_i , y_i , original hashed password $h(PW_i)$, and new hashed password $h(PW_i')$ to the GW.
2. After receiving the password-change request, the GW first decrypts y_i and checks whether $h(PW_i)$ is correct. Then, it compute y_i' :

$$y_i' = E_x(h(x) || ID_i || h(PW_i')) \tag{7}$$

3. The GW sends y_i' back to U_i .
4. U_i updates the smart card with y_i' .

The overall operation of the password-change phase is illustrated in Figure 3.

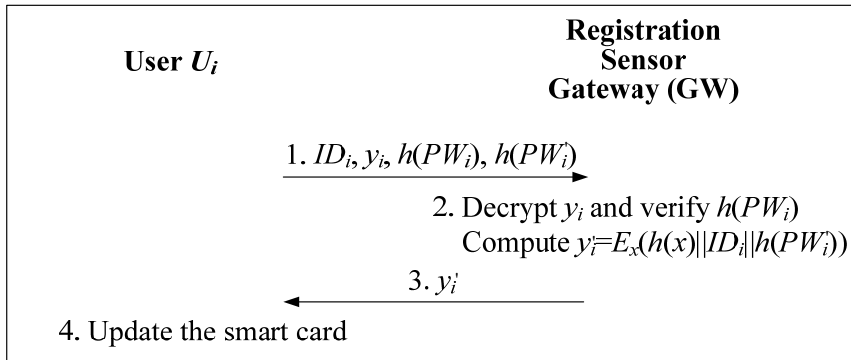


Figure 3. The password-change phase of the proposed scheme.

5. Analysis of Our Scheme

In this section, we shall analyze our scheme and show that it can resist several well-known attacks. In addition, we provide a comparative study with other authentication schemes.

5.1. Functionality

We summarize the functionality of our proposed scheme in this subsection. The crucial criteria in a user authentication scheme are listed below:

- C1. Freely chosen password:** A user can choose his/her password freely in the registration phase.
- C2. Mutual authentication:** Each user and sensor node can authenticate with each other.
- C3. Key agreement:** After successful authentication, users and sensor nodes generate session keys for protecting the subsequent communications.

C4. Secure password change: After the registration, a user can change his/her password freely.

We summarized the functionality of related authentication schemes in Table 2.

Table 2 Comparison of user authentication schemes for WSNs

| | C1 | C2 | C3 | C4 |
|-------------------------------|-----|-----|-----|-----|
| Our proposed scheme | Yes | Yes | Yes | Yes |
| Benenson et al.'s scheme [16] | No | No | No | No |
| Jiang et al.'s scheme [18] | No | Yes | Yes | No |
| Wong et al.'s scheme [19] | Yes | No | No | No |
| Tseng et al.'s scheme [20] | Yes | No | No | Yes |

C1: freely chosen password; C2: mutual authentication; C3: key agreement; C4: secure password change.

5.2. Security Analysis

We will show that the proposal scheme can withstand the following attacks: replay attack, forgery attack, offline-dictionary attack, stolen smart card attack, and insider attack. Mutual authentication will also be considered.

1. **Replay attack:** Assume an attacker re-submits the message C_0 obtained in a previous session. Upon receiving C_0 , the H-sensor randomly chooses v' and then computes C_1' :

$$C_1' = E_u(ID_i || h(u) || v') \quad (8)$$

At this point, the attacker cannot decrypt C_1' since he/she does not have the encryption key u , which was chosen by the legitimate user in the previous session. Therefore, the attacker cannot compute C_2' due to the lack of $h(v')$. As a result, our scheme is secure against the replay attack.

2. **Forgery attack:** Assume an attacker obtains $(ID_i, y_i, h(\cdot), n)$ stored in user i 's smart card and eavesdrops the messages $C_0, C_1,$ and C_2 transmitted between the user and an H-sensor in the login-and-authentication phase in a previous session. Next, the attacker computes w_0' and C_0' :

$$w_0' = (ID_i || y_i || u')^2 \text{ mod } n \quad (9)$$

$$C_0' = (ID_i || w_0') \quad (10)$$

Then, the attacker sends C_0' to the H-sensor. The H-sensor randomly chooses v' and then computes C_1' :

$$C_1' = E_{u'}(ID_i \parallel h(u') \parallel v') \quad (11)$$

However, the attacker cannot mount a forgery attack to masquerade as an authorized user since he/she does not have $h(PW_i^*)$ for constructing C_2' . Hence, the attacker has no chance to log in by launching a forgery attack.

3. **Offline-dictionary attack:** Assume an attacker intercepts the messages C_0 , C_1 , and C_2 transmitted between the user and an H-sensor in the login-and-authentication phase. The attacker cannot perform the offline-dictionary attack to uncover the user's password since the password is encrypted with a secret symmetric key unknown to the attacker. Therefore, the offline-dictionary attack cannot be launched against our scheme.
4. **Stolen smart card attack:** Assume an attacker obtains $(ID_i, y_i, h(\cdot), n)$ stored in user i 's smart card and intercepts the messages C_0 , C_1 , and C_2 transmitted between the user and an H-sensor in the login-and-authentication phase. The attacker cannot decrypt y_i to obtain any secret information about user i since y_i is encrypted with the secret key x , which is known only to the GW and only can be recovered by H-sensors. Obviously, the proposed scheme can prevent the stolen smart card attack. Note that we assume that H-sensors are equipped with tamper-resistant hardware to protect key material.
5. **Insider attack:** In our proposed scheme, when U_i wants to register with the GW for accessing the resources in HSN, he/she has to submit $(ID_i, h(PW_i))$. It is considered practically impossible for the insider to derive the user's password PW_i from the hashed value $h(PW_i)$ [33]. Therefore, the proposed scheme can resist an insider attack.
6. **Mutual authentication:** An attacker cannot impersonate the user or an H-sensor since the attacker cannot obtain the correct u and v , which are randomly chosen by the user and H-sensor in messages C_0 and C_1 , respectively. It turns out that the proposed scheme achieves mutual authentication between a user and the H-sensor.

5.3. Efficiency Analysis

Now we examine the performance of our proposed scheme. The notations are defined in Table 3. The performance of the proposed scheme in the login-and-authentication phase is presented in Table 4. We use the computational overhead as the metric to evaluate the performance of the proposed scheme. The proposed scheme adopts two types of cryptosystems, asymmetric and symmetric. The former is used to protect secret parameters in the smart card, and the latter is used to protect the authentication messages. Compared with Benenson et al.'s scheme, our proposed scheme provides various functionalities with only several extra symmetric encryption and decryption operations.

Table 3 Evaluation parameters

| Symbol | Definition |
|------------|--|
| T_R | The time for performing a random number generation |
| T_H | The time for performing a one-way hash function |
| T_{AENC} | The time for performing an asymmetric encryption operation |
| T_{ADEC} | The time for performing an asymmetric decryption operation |
| T_{SENC} | The time for performing a symmetric encryption operation |
| T_{SDEC} | The time for performing a symmetric decryption operation |

Table 4 Performance comparison of user authentication schemes for WSNs

| Type | Benenson et al.'s scheme | | Proposed scheme | |
|------------|--------------------------|-----------|-----------------|-----------|
| | Each node | Each user | H-sensor | Each user |
| T_R | 1 | 0 | 1 | 1 |
| T_H | 1 | n^* | 3 | 4 |
| T_{AENC} | 0 | n | 0 | 1 |
| T_{ADEC} | 2 | 0 | 1 | 0 |
| T_{SENC} | 0 | 0 | 1 | 1 |
| T_{SDEC} | 0 | 0 | 2 | 1 |

n^* : Assume there are n sensors in the communication range of the user.

6. Conclusions

In this paper, we proposed a robust password-based authentication scheme for HSNs. The scheme provides not only mutual authentication but also key agreement between a user and a sensor node and adopts fuzzy identity-based encryption for gateway nodes and high-end sensor nodes in HSNs. Our analysis shows that the proposed scheme is immune to many notorious attacks, including replay attacks, forgery attacks, offline-dictionary attacks, stolen smart card attacks, insider attacks, and many other potential breaches of security. An area of future research that should be considered is to combine biometrics and passwords for the purpose of raising the security level.

References

- [1] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers and Security*, vol. 21, no. 4, Aug. 2002, pp. 372-375.
- [2] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," *ACM SIGOPS Operating Systems Review*, vol. 36, no. 4, Oct. 2002, pp. 23-29.
- [3] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, May 2003, pp.

414-416.

- [4] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, Nov. 2003, pp. 1243-1245.
- [5] W. S. Juang, "Efficient password authenticated key agreement using smart cards," *Computers and Security*, vol. 23, no. 2, Mar. 2004, pp. 167-173.
- [6] C. L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 26, no. 3, May 2004, pp. 167-169.
- [7] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic id-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, May 2004, pp. 629-631.
- [8] A. Awasthi, "Comments on a dynamic id-based remote user authentication scheme," *Transactions on Cryptology*, vol. 1, no. 2, Aug. 2004, pp. 15-17.
- [9] C. Y. Lee, C. H. Lin, and C. C. Chang, "An improved low computation cost user authentication scheme for mobile communications," In *Proceedings of the IEEE International Conference on Advanced Information Networking and Applications (AINA 2005)*, vol. 2, Mar. 2005, pp. 249-252.
- [10] I. E. Liao, C. C. Lee, and M. S. Hwang, "Security enhancement for a dynamic id-based remote user authentication scheme," In *Proceedings of the IEEE International Conference on Next Generation Web Services Practices (NWeSP 2005)*, Aug. 2005, pp. 22-26.
- [11] C. L. Hsu, "A user friendly remote authentication scheme with smart cards against impersonation attacks," *Applied Mathematics and Computation*, vol. 170, no. 1, Nov. 2005, pp. 135-143.
- [12] S. W. Lee, H. S. Kim, and K. Y. Yoo, "Improvement of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 27, no. 2, Jan. 2005, pp. 181-183.
- [13] Y. Lee, J. Nam, S. Kim, and D. Won, "Two efficient and secure authentication schemes using smart cards," In *Proceedings of International Conference on Computational Science and its Applications (ICCSA 2006)*, May. 2006, pp. 858-866.
- [14] H. T. Liaw, J. F. Lin, and W. C. Wu, "An efficient and complete remote user authentication scheme using smart card," *Mathematical and Computer Modelling*, vol. 44, no. 1-2, Jul. 2006, pp. 223-228.
- [15] Z. Benenson, F. Gärtner, and D. Kesdogan, "User authentication in sensor networks (extended abstract)," In *Proceedings of Informatik 2004, Workshop on Sensor Networks*, Sept. 2004.
- [16] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authentication in sensor networks," *Workshop on Real-World Wireless Sensor Networks (REALWSN 2005)*, Jun. 2005.
- [17] H. Wang and Q. Li, "Distributed user access control in sensor networks," In *Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, Jun. 2006, pp. 305-320.
- [18] C. Jiang, B. Li, and H. Xu, "An efficient scheme for user authentication in wireless sensor

- networks,” In *Proceedings of the IEEE International Conference on Advanced Information Networking and Applications Workshops (AINAW '07)*, May 2007, pp. 438-442.
- [19] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks,” In *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC '06)*, vol. 1, Jun. 2006, pp. 244-251.
- [20] 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 2007)*, Nov. 2007, pp. 986-990.
- [21] P. Gupta and P. R. Kumar, “The capacity of wireless networks,” *IEEE Transactions on Information Theory*, vol. 46, no. 2, Mar. 2000, pp. 388-404.
- [22] E. J. Duarte-Melo and M. Liu, “Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks,” In *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2002)*, Nov. 2002, pp. 21-25.
- [23] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, “Exploiting heterogeneity in sensor networks,” In *Proceedings of the IEEE INFOCOM*, Mar. 2005, pp. 878-890.
- [24] X. Du and Y. Xiao, “Energy efficient Chessboard Clustering and routing in heterogeneous sensor networks,” *International Journal of Wireless and Mobile Computing*, vol. 1, no. 2, 2006, pp. 121-130.
- [25] X. Du and F. Lin, “Maintaining differentiated coverage in heterogeneous sensor networks,” *EURASIP Journal on Wireless Communications and Networking*, no. 4, 2005, pp. 565-572.
- [26] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, “An effective key management scheme for heterogeneous sensor networks,” *Ad Hoc Networks*, vol. 5, no. 1, Jan. 2007, pp. 24-34.
- [27] J. Brown, X. Du, and K. Nygard, “An efficient public-key-based heterogeneous sensor network key distribution scheme,” In *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2007)*, Nov. 2007, pp. 991-995.
- [28] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” *Advances in Cryptology - EUROCRYPT 2005*, May 2005, pp. 457-473.
- [29] J. Baek, W. Susilo, and J. Zhou, “New constructions of fuzzy identity-based encryption,” In *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS '07)*, Mar. 2007, pp. 368-370.
- [30] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, Oct. 2006, pp. 89-98.
- [31] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,” In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, Oct. 2006, pp. 99-112.
- [32] M. O. Rabin, “Digitalized signatures and public-key functions as intractable as factorizations,” *Technical Report*, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass. Jan.

1979.

[33] B. Schneier, *Applied Cryptography*, John Wiley & Sons Inc., New York, 2nd edition, 1996.