Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 407971, 13 pages
http://dx.doi.org/10.1155/2013/407971

Research Article

An Efficient Biometric Authentication Protocol for Wireless Sensor Networks

Ohood Althobaiti, Mznah Al-Rodhaan, and Abdullah Al-Dhelaan

Computer Science Department, King Saud University, Riyadh, Saudi Arabia

Correspondence should be addressed to Mznah Al-Rodhaan; rodhaan@ksu.edu.sa

Received 25 January 2013; Accepted 20 April 2013

Academic Editor: Muhammad Khurram Khan

Wireless sensor networks (WSNs) are spreading rapidly due to their flexibility to communicate which demands a secure environment. The most important requirements of WSN security are confidentiality, authentication, and integrity. User authentication is necessary for legitimate access control in WSNs. Sensors have limited processing power, bandwidth, memory, and limited communication abilities. Significantly, the system must produce an authentication method to confirme if the user is legal or not. In this paper, we present a solution based on biometric and adapt it for a WSN environment. The proposed protocol involves simple operations and light computations. The main advantage of the proposed protocol is using the user's iris to regenerate the user's key on-the-fly every time the user wants be authenticated which dramatically enhances security aspects in WSNs. The key used in this protocol is stronger than passwords and shorter than biometric data, which balances between security and performance. Our protocol uses much light computations and simple operations in both homogenous and heterogeneous environments; therefore, it is suitable to the WSNs.

1. Introduction

Wireless sensor network (WSN) collects the observed data about an environment over a certain geographic area [1]. Users can request and watch the data when they need it (ad hoc queries) or when an event has been triggered.

Very soon, the environmental data will be omnipresent. The reason behind that are the pervasive nature of WSN and its simplicity of deployment which helps in proposing various types of WSN implementations. Such usage of a WSN for smart constructions and the prediction of heat and dampness measurements in a specific position of an area will be on request. Commonly, the great number of requests in WSN implementations is processed at the gateway or the base station points. Nevertheless, we could predict the increasing of higher requests to reach the real-time data from WSNs. This will prevent the real-time data from being reached just at the gateway nodes or at the base stations, rather it could be reached from a sensor node of a WSN in an ad hoc way. Nonetheless, in several situations the use of such gateway node or base station is impossible or not achievable forcing the user to access the sensor devices directly. For instance, data might be located in the directly accessed nodes. In such situation, inquiries and data dissemination have to be performed through the WSN for security purposes. For example, the temporary deployment in battlefield or area where there is no existing network infrastructure is the situation with deployment deep in desert or forest.

The collected data might not be critical (e.g., the humidity in a specific location inside a house), while in some cases they might be confidential and valuable. In the latter case, some security measures must be considered to protect these critical data and not to allow the accessibility of unauthorized users to reach these data. One of the well-known problems in most of the available computer applications and systems is the access control. One of the primary solutions is the user authentication which used to prove the identity of user or a machine as client to access the system or application. User authentication examples can be faced regularly, like entering a local area network of our work place, verification of hand phone appliances, down to the verification of our account transaction of ATM machines, and so on. Nevertheless, a great effort has been done on WSN security

but there are many opened issues that need to be tickled taking into consideration the nature of resource constraints of WSN such as computation limitations, storage, and battery power. It is very challenging to implement the traditional solution of user authentication for wired environments to WSNs.

In this paper, we will discuss the problem of the user authentication in the context of WSNs since a legal user is permitted to query the data in an ad hoc way from any sensor node within WSN and present the needed literature review in Section 2. Furthermore, we suggest a biometric-based user authentication protocol in Section 3. Moreover, Section 4 analyses the security aspects of our protocol. In Section 5, we analyse the protocol performance using analytical modeling. Performance evaluation for the proposed protocol using simulator is presented in Section 6, while Section 7 concludes our study.

2. Literature Review

In a WSN application layer, many security protocols were applied to enhance the security of the layer efficiently, since the standard security protocols in an application layer are considered not strong enough for many information systems privacy [2]. In [3], Benenson et al. propose a user authentication protocol which is used to handle node capture attack. This protocol needs exponential computations because of their protocol based on elliptic curve discrete logarithm problem (ECDLP). As a result, the computational time of Benenson et al.'s protocol is high because exponential computations are expensive. Also, this protocol relies on the existence of a trusted third party.

In 2006, Wong et al. [4] has proposed a dynamic WSN authentication scheme based on a light-weight strong password. This scheme involves three phases: registration phase, login phase, and authentication phase. However, Wong et al.'s scheme has three main advantages that are discussed as follows.

(i) It gives the authorized users privilege to access data at any sensor nodes in an ad hoc method.

(ii) It reduces the computation cost by loading very little operations.

(iii) It is secure enough against some of replay/forgery attacks.

Whereby, this scheme has four disadvantages.

(i) It has some weakness in protecting against all replay/forgery attacks.

(ii) Sometimes sensor node reveals and exposes the password information to other nodes.

(iii) It does not allow users to change their password freely.

(iv) The scheme is always vulnerable to stolen-verifier threats.

Tseng et al. [5] have improved Wong et al.'s scheme by fixing the security weakness in it. This improvement has been designed by adding an extra phase on Wong et al. phases. However, Tseng et al.'s scheme has four phases: registration, login, authentication, and password changing phase.

Novelty, Ko [6] showed that the authentication process shown in [5] is still insecure and does not achieve mutual authentication, which is very important for many applications. Moreover, Vaidya et al. [7] highlighted other weaknesses on Tseng et al., Wong et al., and Ko schemes. Vaidya et al. pointed out that the previous mentioned schemes are still not strong enough to protect against some attacks such as replay of account login, stolen verifier, and man-in-the-middle attacks. Vaidya et al. enhanced the security by proposing two WSN authentication schemes depending on the traditional password authentication schemes.

However, Das [8] has also highlighted the weakness of Wong et al. against stolen-verifier attacks, as well as identified two-factor user authentication scheme for WSN which is based on password and smart card. Although this two-factor scheme can be used to protect networks but it requires some complicated equipment.

In [9], He et al. have developed and discussed two-factor authentication scheme. This development is proposed to enhance the security of the two-factor scheme by dividing their scheme into three main phases: registration, authentication, and password-changing phase.

However, He et al. have developed another issue from Das's scheme. This developed issue is still suffering from some security limitations, such as session key establishment (where the session key between user and node sensor is not established after authentication phase in the developed scheme) and authentication process between user and sensor node.

Consequently, Nyang and Lee [10] showed that Das's scheme is still vulnerable and has some security weakness in offline-password-guessing attacks. As a result, Das's scheme cannot control and protect the established query-response messages between sensor node and user. Therefore, Nyang and Lee proposed a scheme to overcome the important security weakness in Das's scheme.

Khan and Alghathbar [11] studied Das's scheme in more details. They mentioned that Das's scheme is still vulnerable to several types of attack, since Das's scheme does not provide some features such as password changing and gateway and sensor mutual authentication. Therefore, their suggestions to fix this weakness are by adding password changing phase and providing gateway/sensor mutual authentication phase. The suggested scheme is still weak because of the limitations on the session key establishment between the user and sensor node in WSN.

Arikumar and Thirumoorthy [12] proposed their contribution in securing WSN depending on the two-factor authentication scheme and nonpublic key operations such as hash function. This contributed scheme prevents users who have the same identity from logging into the system.

Yeh et al. [13] presented a new user authentication scheme depending on elliptic curve cryptosystem and smart card authentication method. This contribution is still weak in the following regards.

(i) Communication cost is very expensive compared to the existing schemes.

(ii) Working without user/sensor node mutual authentication.

(iii) Working without key sharing between the user and the sensor node.

Recently, Yuan et al. [14] used biometric approach to propose their user authentication scheme in WSN. In addition, they used password and smart card in their presented work. After Yuan et al.'s biometric scheme, Yoon and Yoo [15] proposed a new user authentication protocol based on biometric approach and without using password. They also showed the message integrity problem in Yuan et al.'s scheme. Although they suggested security improvements of Yuan et al.'s protocol, but some drawbacks are still in their protocol, for example, there is no session key established after authentication between the sensor node and the user, and no confidentiality of messages is considered; also their protocol requires some complicated equipment and is still vulnerable to several types of attack such as denial of service (DoS) attack.

3. Proposed Protocol

We observed that the existing protocols have security weaknesses, such as, DoS, man-in-the-middle attack (MIMA), and guessing attack. No confidentiality of messages is considered and may require some complicated equipment. We suggest security improvements in our protocol to fix some of the drawbacks to improve the existing user authentication in WSNs. Our protocol not only solves the aforementioned drawbacks but also improves the security of user authentication in WSNs.

Our user authentication protocol is based on biometric encryption and hash function which is feasible for WSNs without special hardware support (i.e., without additional equipment) and without third party. Moreover, our protocol is suitable for large scale applications.

The main advantage which dramatically enhances security aspects in WSNs is that the user's iris is used to regenerate the user's key on-the-fly every time the user wants to be authenticated. This encryption key is shorter than biometric data and stronger than a password, that balances the tradeoff between performance and required security; it becomes possible to achieve biometric-based user authentication without transmitting and saving any private information anywhere (i.e., no need to store neither images nor the template of them in the memory. The encryption key and the image or template of image must be discarded at the end of the registration phase).

Our major goal is to decrease possible problems which are caused by illegal users. So we suggest a user authentication protocol to fulfill the following requirements.

(i) Our protocol provides protection against main attacks in WSNs such as replay attack, impersonation attack, MIMA, stolen-verifier attack, repudiation attack, data corruption attack, password guessing attack, and DoS attack. The security of conventional user authentication protocols is founded on password. Short password is broken without difficulty using password guessing attacks. Furthermore, a password can be shared with other people or be lost so there is no method to know who is the real user. Biometric encryption can solve the above security problems, that is, based on behavioral or physiological characteristics of persons, for example, fingerprints, iris scan, faces, hand geometry, vein patterns, voice patterns, and so forth. The biometric-based authentication is more reliable than conventional authentication based on a password.

(ii) Our protocol provides mutual authentication between not only gateway and sensor node but also between gateway and user.

(iii) Our protocol was adapted to be efficient and lightweight in terms of computational cost and communication cost to decrease the energy consumption of sensor nodes which have limited energy and resources.

(iv) Our protocol is based on a zero-knowledge proof. This means that it allows a claimant to prove the knowledge of a secret without revealing it.

(v) Our protocol provides confidentiality of messages between all entities (user, gateway, and sensor node); therefore, only authorized users can use these messages, which are confidential against any attack.

The proposed protocol uses iris encryption in user authentication for wireless sensor networks. In this protocol, there are four main phases: registration, login, authentication, and user's key change. We chose iris scan as the most appropriate personnel trait for authenticating users, because it was demonstrated that iris is one of the most accurate traits for user authentication. Other advantages for authentication based on iris scan are found in the literature [16]. Moreover, iris authentication may need no additional hardware on the user devices with the presence of digital cameras now are included in most computer devices [17]. The number of commercial software produces iris recognition using mobile devices cameras, for example, BioWallet on Android and OKI's iris recognition on Symbian.

We have made the following assumptions for user authentication.

(i) The gateway node (GW-node) or base station (BS) is considered as trusted node.

(ii) Each user must register in the system once to access the WSN data.

The notations used in the protocol are explained in Table 1.

After extracting the iris's features, the biometric encryption will take place by using a fuzzy commitment scheme, as in [17]. Fuzzy commitment scheme overcomes the drawback of traditional biometric systems where there is no need to store neither images nor the template of them in the memory.

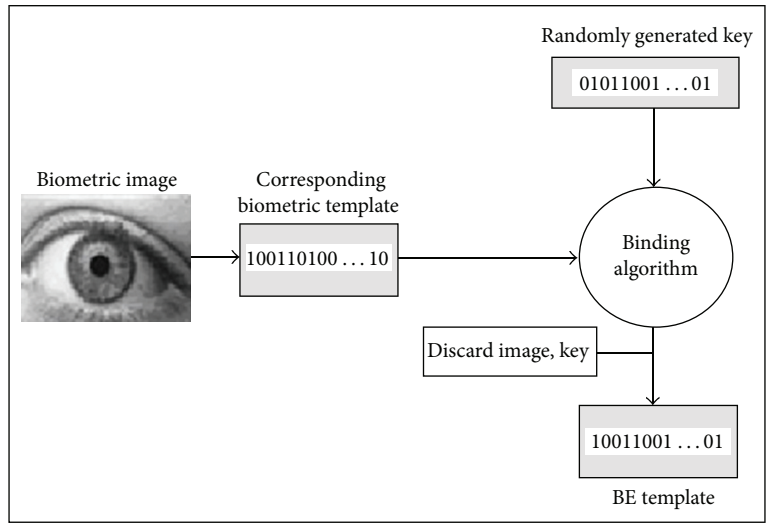

Figure 1: Biometric cryptography.

Table 1: Notations used in the protocol.

Notation	Meaning
U	User
SN	Identity of sensor login-node N, that is, nearest sensor node of WSN
ID	User's identity
$h(\cdot)$	One-way Hash function
$\|$	Concatenation
$E_{\text{key}}(m)$	Message m is encrypted with secret key
$D_{\text{key}}(m)$	Message m is decrypted with secret key
$\text{MAC}_{\text{key}}(m)$	Message authentication code

Biometric data has a variable nature and the encryption needs an exact key to work well; so before biometric data can be used as a key for encryption, its representation must be stabilized. Error-correction codes are used for the stabilization process [17].

Registration phase of our protocol is performed by extracting the features of iris using an iris recognition system, then binding (XORing) the corrected biometric data with a random generated key (user's key). Then the biometric encryption (BE) template will be saved in the user's device (PDA/PC).

Additionally, the hash value of encryption key will be saved with the BE template to be able to reject incorrect keys in an early step, before beginning the process of remote authentication as shown in Figure 1.

When the BE template is saved in the user's device, the user can retrieve his key by capturing an image of his iris via the user's device camera. After that, the features of iris will be extracted by the iris recognition model, then XORed with the BE template to regenerate the user's key as shown in Figure 2.

There are two methods to authenticate the user using the biometric encryption. One of them uses the biometric to create a pair of private and public key, as proposed by [16], and publish the public key. The other method uses biometric encryption to generate a user's secret key [18]. The problem in the second method is the decision of what should be saved on the GW-node/BS to authenticate the user. The first answer is the "BE template," as it is in a normal biometric authentication. Unluckily, this is not useful from the viewpoint of the biometric, because the user must transmit his/her biometric data to the remote authenticator for retrieving his/her key from the GW-node database. The best solution is that the key of user is saved on the GW node. Although this solution contradicts with the biometric encryption aim to not save the key of user, but this inconsistency will be on the GW-node side only which has a high level of security, particularly if the users' keys were encrypted in the GW-node database. Hence, the security of the GW-node is not the matter because this method is similar to the well-known Kerberos protocol. Furthermore, if the user's key is stolen, it can be simply revoked using the reenrollment process. We use the second method for our user authentication protocol because the symmetric cryptographic is less complex than asymmetric cryptography and consumes less resources, which is an important issue in limited resources devices, for example, sensor node and mobile devices.

3.1. Registration Phase. When the user U_i registers in the system, an encryption key will be generated randomly for U_i. The generated key is saved on the GW node as a key of U_i. After that, the features of the U_i's iris are extracted then hashed by SHA256 [17], then the hash is XORed with the key to generate a BE template which will be saved in the U_i's device to use it for the authentication phase to regenerate the key from the U_i's iris. The template of iris is large, also if we use a part of the iris template in the biometric encryption that is not secured enough, so the hash was used because a fixed size output for variable length inputs is produced by the hash function and the hash function is collision resistant. Additionally, the hash of the key will be saved with the BE template to be able to reject incorrect keys in an early step,

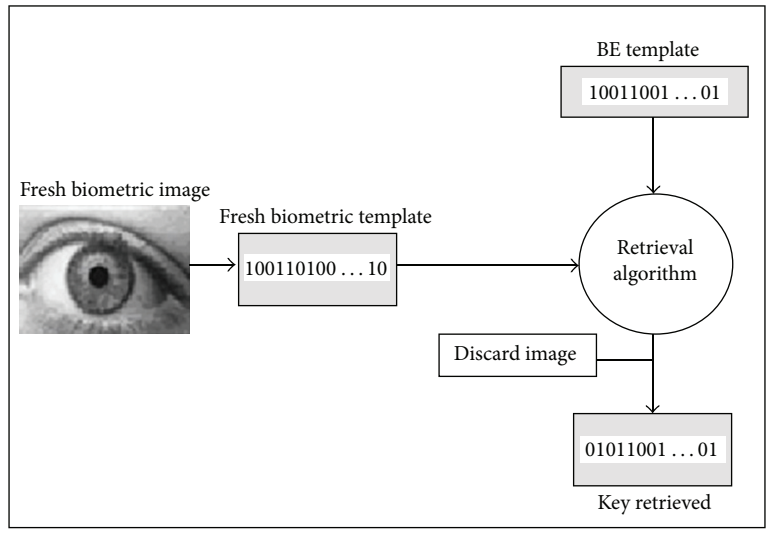

Figure 2: Decrypt with same biometric.

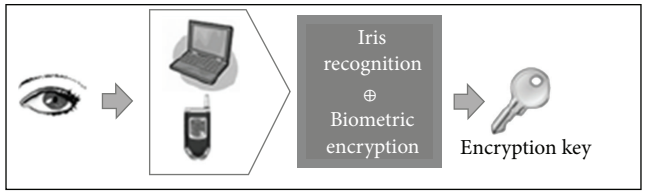

Figure 3: Login phase.

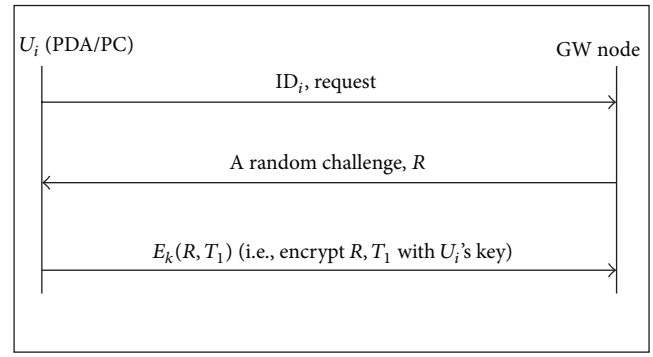

Figure 4: Authentication between user U_i and GW node.

before beginning the procedure of remote authentication. The U_i data (ID_i, name, etc.) and the encryption key of the U_i are saved in the GW-node database. After that, the GW node sends to the U_i an ID_i and $F_i = h(ID_i \oplus X)$ through a secure channel to utilize them at an authentication phase to authenticate himself. Where X is a secret parameter which is generated by the GW-node and it is saved in all the SNs (the sensor login-nodes) before the nodes are deployed in the field. These sensor nodes (SNs) will be responsible to respond to the data/query that users are looking for and know X.

3.2. Login Phase. After iris acquisition by camera in the U_i's device, the features of U_i's iris are extracted. After that, the iris's features are corrected by error correcting code and hashed by SHA256. Then, the hash of corrected iris's features is XORed with the saved BE template to regenerate the U_i's key as in Figure 3. Then, the U_i's key is hashed, and this hash will be compared with the saved hash of the U_i's key. If the two hashes are not equal, the remote authentication is aborted. If they are equal, the application is proceeded. After that, a request is sent to the GW node including the user ID_i.

3.3. Authentication Phase. When GW node receives the login request, it replies with a random challenge R. Here the GW node would challenge the user to encrypt a bit of known information using the encryption key. When the user receives the GW-node response, he/she will encrypt R and T_1, where T_1 denotes the current timestamp of the U_i's device, using the encryption key which is generated from the iris template and sent the encrypted message to GW node. When GW node receives encrypted message at time T_2, it will decrypt this message using the key of U_i then checks the freshness of timestamp T_1 as in Figure 4. If $(T_2 - T_1) > \Delta T$, the authentication phase will be aborted, where ΔT denotes interval of the expected time for the transmission delay in the WSN. In contrast, if $(T_2 - T_1) \leq \Delta T$, the following steps will be achieved.

The next step is that GW node computes $F_i = h(ID_i \oplus X)$, then computes $Y_i = MAC_{F_i}(ID_i \parallel SN \parallel T_3)$, where SN denotes the sensor node which will reply to the query with what U_i is looking for and T_3 denotes the GW node's current timestamp. The GW node transmits a message (ID_i, Y_i, T_3) to the SN over a public channel. Y_i used by SN to ensure that the message (ID_i, Y_i, T_3) issues from the legal GW node since Y_i is produced using X, that is known to the GW node and SN.

When the request is received by the SN at time T_4, it will carry out the following steps, the verification of T_3. If $(T_4 - T_3) > \Delta T$, the authentication phase will be aborted, where

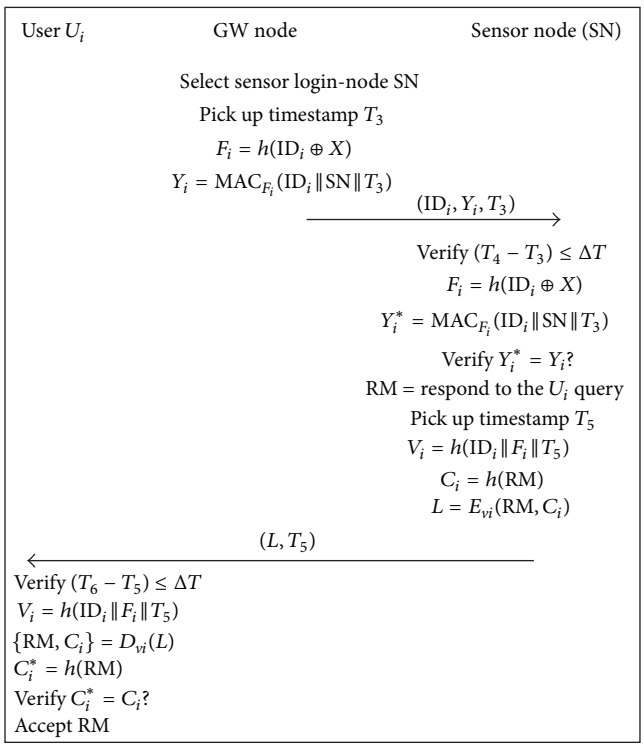

Figure 5: Authentication phase.

ΔT denotes interval of the expected time for the transmission delay in the WSN. In contrast, if $(T_4 - T_3) \le \Delta T$, the following step will be achieved. The SN computes $F_i = h(\mathrm{ID}_i \oplus X)$ and $Y_i^* = \mathrm{MAC}_{F_i}(\mathrm{ID}_i \| \mathrm{SN} \| T_3)$; after that, it verifies whether or not Y_i^* is equal to Y_i. If the previous two verifications successfully pass, the SN sets respond to the U_i query (RM), then compute $V_i = h(\mathrm{ID}_i \| F_i \| T_5)$ and $C_i = h(\mathrm{RM})$, where T_5 denotes the sensor node's current timestamp, then compute $L = E_{vi}(\mathrm{RM}, C_i)$ (i.e., SN encrypts RM and C_i with V_i); after that, the SN sends a message (L, T_5) to the U_i.

In next step, when the U_i receives the message (L, T_5) at time T_6, U_i verifies from freshness of timestamp T_5. If $(T_6 - T_5) > \Delta T$, the authentication phase will be aborted. In contrast, if $(T_6 - T_5) \le \Delta T$, U_i computes $V_i = h(\mathrm{ID}_i \| F_i \| T_5)$ and then decrypts the message L with V_i (i.e., U_i computes $D_{vi}(L)$) to get RM and C_i and then computes $C_i^* = h(\mathrm{RM})$; after that, he/she verifies whether or not C_i^* is equal to C_i. If the previous steps successfully pass, the U_i will accept the RM as explained in Figure 5. Furthermore, the SN and U_i have become the shared session key $V_i = h(\mathrm{ID}_i \| F_i \| T_5)$; this session key can be used to achieve more operations during a session. Therefore, a legal user communicates to sensor nodes in an ad hoc way to access data of the WSN.

3.4. User's Key Change Phase. According to the proposed protocol, the user's key can be changed by re-enrollment process. When the key is compromised, U_i can do re-enrollment by his/her biometric, and then a new key is generated randomly; this key differs from the previous.

4. Security Analysis Using Threat Model

This section proves our protocol's strength in terms of security. We demonstrate that the proposed protocol resists main types of attacks in WSNs which are found in the literature.

In communication networks, the threat model is employed to analyze crypto protocols formally, since the threat model assumes that two parties can communicate over an insecure channel. WSNs can adopt the threat model where the channel of communication between two parties is insecure, and the end points (sensor node and user) cannot be trusted generally.

Proclamation 1. The proposed protocol resists a DoS attack.

Proof. The DoS attack in the existing user authentication protocols can be occurred by attacker who is transmitting the large number of requests to GW node in login and authentication phases to make the GW node fail. Our protocol prevents DoS attack by preauthentication, since each request should associate with timestamp T_1 encrypted by the U_i's key; for this reason, a large number of unauthorized requests cannot get into the GW node.

$U_i \rightarrow$ GW-node: preauthentication $= E_K(R, T_1)$, where T_1 denotes the current timestamp of the U_i's device. □

Proclamation 2. The proposed protocol provides confidentiality of messages between all entities (user, gateway, and sensor node).

Proof. Messages confidentiality against eavesdropping attack are performed by data encryption service. Our protocol can provide sufficient confidentiality for transmitted messages (e.g., $E_K(R, T_1)$ and $L = E_{vi}(\mathrm{RM}, C_i)$). More specifically, these messages are confidential against any adversary. If data is sent without encryption over a public channel, the attacker is able to view the plaintext data as it passes over the network; this attack occurs in Yoon and Yoo's protocol [15], where in [15] the sensor node's responding message (RM) is sent to the user over a public channel without encryption. □

Proclamation 3. The proposed protocol resists a node compromise attack.

Proof. WSNs are normally deployed in an unattended environment. The attacker can easily capture a sensor node (SN) and attempt to collect some secret information about the network from this sensor node. Implementation of one-time sensors prevents this type of the attack, but it is limited to some applications (e.g., fire alarm), because the data confidentiality is not important. When the data confidentiality is important, it is a difficult task to prevent this type of the attack if sensor nodes are not tamper-proof and the environment is hostile and unattended. However, the GW node can periodically monitor whether any sensor node is captured or not. If authentication of user and data access from sensor node are allowed directly to the user (i.e., without GW node's notice) then the effect of "node compromise" attack

is very high, which occurs in Watro et al.'s scheme [19]. But in our protocol, the user's request is first authenticated by the GW node and after that the request is transmitted to the sensor node to respond to the user query. □

Proclamation 4. The proposed protocol resists a replay attack.

Proof. As a rule, if previously obtained information is not reusable, then replay attacks are impossible [20]. When an opponent eavesdrops on the communication between the U_i and the GW node, he/she only gets encrypted data (unreadable form), which is not reusable. Therefore, no opponents's success replay attacks on the proposed protocol.

The timestamps T_i ($i = 1, 2, \ldots, 6$) are used in the suggested protocol to prevent the replay attack. If an adversary intercepts the message $E_K(R, T_1)$ and attempts replaying the same message for login to the GW node, he/she cannot pass the verification of the login request because of $(T_2 - T_1) > \Delta T$, where T_2 denotes the time when the replayed message is received by the GW node. Similarly if an adversary intercepts $(\mathrm{ID}_i, Y_i, T_3)$ and attempts replaying the same message, he/she cannot pass the verification of the login request because of $(T_4 - T_3) > \Delta T$. Also if an adversary intercepts (L, T_5) and attempts replaying the same message, he/she cannot pass the verification of the login request because of $(T_6 - T_5) > \Delta T$. □

Proclamation 5. The proposed protocol resists an impersonation attack.

Proof. The suggested protocol resists impersonation attack since an adversary may intercept a login request $E_K(R, T_1)$, nevertheless, to log in again, $E_K(R, T_1)$ must be recomputed by using a new timestamp T_{new}, for avoiding the replay attacks. This is impossible without U_i's iris since U_i's iris is required to regenerate the U_i's key, and the user's biometrics cannot be attained by the adversary. Therefore, the adversary cannot achieve impersonate attack. Therefore, the proposed scheme can resist user impersonation attack. Also the adversary cannot impersonate a valid GW node. Assume that an adversary intercepts a valid login message $(\mathrm{ID}_i, Y_i, T_3)$ to impersonate a valid GW-node. Nevertheless; because the MAC function must be one way where MAC function must be hard to invert (i.e., given random $y \in \{0, 1\}^n$, hard to find any x such that $h(x) = y$), the adversary cannot extract secret value $F_i = h(\mathrm{ID}_i \oplus X)$ from $Y_i = \mathrm{MAC}_{F_i}(\mathrm{ID}_i \parallel \mathrm{SN} \parallel T_3)$. Without knowing F_i, the adversary cannot perform the GW-node impersonation attack since the adversary cannot make a new message $(\mathrm{ID}_i, Y_i^{\mathrm{new}}, T_{\mathrm{new}})$, where $Y_i^{\mathrm{new}} = \mathrm{MAC}_{F_i}(\mathrm{ID}_i \parallel \mathrm{SN} \parallel T_{\mathrm{new}})$ and T_{new} denotes a timestamp of the adversary. Consequently, the suggested protocol resists the GW-node impersonation attack. For the same reason, the adversary cannot impersonate a valid sensor node (SN) without knowing the secret value F_i since he/she cannot obtain F_i from the intercepted value $L = E_{vi}(\mathrm{RM}, C_i)$ where $V_i = h(\mathrm{ID}_i \parallel F_i \parallel T_5)$. □

Proclamation 6. The proposed protocol resists a stolen verifier attack.

Proof. The attackers who have stolen the users' keys from GW node cannot obtain any useful information, because the users' keys were encrypted in the GW-node database. □

Proclamation 7. The proposed protocol resists guessing attacks.

Proof. This type of attack is a serious concern in systems based on password. The suggested protocol resists password guessing attacks, because the password of user is not required to login to the WSN. Also the suggested protocol resists the biometric guessing attacks, because our protocol does not require transmitting and saving any private information anywhere. In other words, no preservation of the biometric template or image is done. The best practice from a privacy point of view, in the first place, is not to collect any personally identifiable information (PII) to a completely and fully possible capacity. This is known as "data minimization" which means to minimize the quantity of personal data that are possessed and collected; in this manner, it eradicates the likely preceding abuse. The retention and wrong usage of biometric data are considered as the main reasons of driving most concerns of privacy and security. These threats and concerns are addressed by biometric encryption. □

Proclamation 8. The proposed protocol resists a repudiation attack.

Proof. This type of attack indicates to participation denial in all of the communication or part of it. Our protocol requires U_i's iris to regenerate the U_i's key; therefore, the U_i cannot deny that he/she performed a specific participation; also we assume the GW node is considered as trusted node; thus, our protocol resists a repudiation attacks. □

Proclamation 9. The proposed protocol can resist an integrity threat.

Proof. Data integrity threats faced by our protocol are as follows:

(i) data modification attack,

(ii) data corruption attack,

(iii) data insertion attack.

Integrity is a service used to guarantee that the transmitted data has not been modified via an unauthorized entity. Our protocol can resist integrity threats, since $Y_i = \mathrm{MAC}_{F_i}(\mathrm{ID}_i \parallel \mathrm{SN} \parallel T_3)$ and $C_i = h(\mathrm{RM})$ could be used to protect against integrity threats. The sensor node (SN) can guarantee that the message $(\mathrm{ID}_i, Y_i, T_3)$ has not been modified via an unauthorized entity by recomputing MAC and verifies whether it is equal to the MAC attached to the message. Also the U_i can guarantee that the message (L, T_5) has not been modified via an unauthorized entity by recomputing $h(\mathrm{RM})$ and verifies whether it is equal to the $h(\mathrm{RM})$ attached to the message. □

Proclamation 10. The proposed protocol resists an insider attack.

Table 2: Comparison among representative protocols and our protocol.

	Benenson et al.'s protocol	Yuan et al.'s protocol	Yoon et al.'s protocol	Our protocol
Stolen-verifier attacks	Secure	Secure	Secure	Secure
Guessing attacks	Secure	Secure	Secure	Secure
Impersonation attacks	Insecure	Insecure	Secure	Secure
Replay attacks	Secure	Secure	Secure	Secure
Insider attack	Secure	Insecure	Secure	Secure
Repudiation attack	Secure	Secure	Secure	Secure
Node compromise attack	Secure	Insecure	Insecure	Secure
Denial-of-service attack	Insecure	Insecure	Insecure	Secure
Message confidentiality	Not provided	Not provided	Not provided	Provided
Password change	Not required	Required	Not required	Not required
Key revocability	Not provided	Not provided	Not provided	Provided
Complicated equipment	Not required	Required	Required	Not required
Session key establishment	Not provided	Not provided	Not provided	Provided
Mutual authentication	Not provided	Not provided	Provided	Provided
Data integrity	Not provided	Not provided	Provided	Provided

Proof. An insider attack is intentionally misused by authorized parties. Our protocol aims to achieve biometric-based user authentication without transmitting and saving any private information anywhere (i.e., no need to store the template of image or image in the memory). The encryption key and the image or template of image must be discarded at the end of the registration phase, since only the BE template will be saved in the U_i's device to use it for the authentication phase to regenerate the key from the U_i's iris. For this reason, any insider attack cannot get the correct biometric and cannot get the correct user's key from the BE template because of the advantages of biometric encryption and the one-way hash function. Also the users' keys were encrypted in the GW-node database.

Table 2 shows the functionality comparisons between our protocol and related protocols. According to Table 2, our protocol not only presents confidentiality of messages but also performs all security requirements and without complicated equipment. From the above descriptions, we conclude that our protocol is more practical than the related protocols. □

5. Analytical-Based Performance Evaluation

In this section, we analyze the performance of our protocol based on a mathematical model and compare with the ones in the literature. We employ the computational overhead (denoted by T) to study the performance. The computation time required by each security primitives as stated by practical implementations on Mica2 motes [21] is recorded in Table 3. The total computational cost of our protocol, Benenson et al.'s protocol, Yuan et al.'s protocol, and Yoon et al.'s protocol is shown in Table 4. We calculate the computational time for registration phase separately because the computational time for registration phase is a one-time task at some period. From Table 4, Benenson et al.'s protocol needs exponential computations because their protocol-based on ECDLP. As a result, the computational time of Benenson et al.'s protocol is the highest among the four protocols because exponential computations are expensive.

Table 3: Execution times on Mica2.

Notation	Description	Time (ms)
T_H	Time for performing one-way hash function (SHA-1)	3.636
T_{MAC}	Time for performing MAC function (HMAC-SHA1)	3.12
T_{RC5}	Time to encrypt/decrypt using RC5	0.26

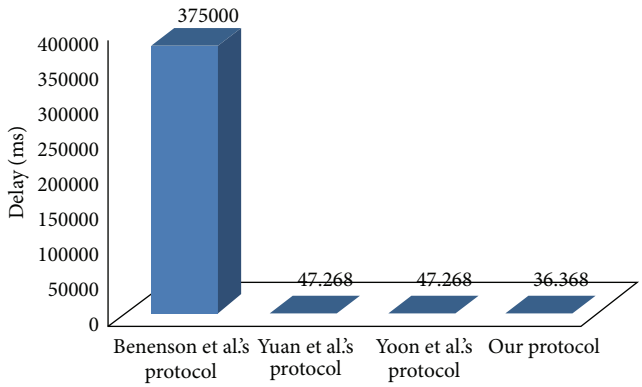

Figure 6: Delay performance.

Also, Benenson et al.'s protocol relies on the existence of a trusted third party while we only assume that the GW node is trusted. Briefly, we minimize the computational time and avoid the want for a trusted third party. Based on Table 4, our protocol requires only 36.368 ms, which is less than Benenson et al.'s protocol (375000 ms), Yuan et al.'s protocol (47.268 ms), and Yoon et al.'s protocol (47.268 ms) as explained in Figure 6.

Table 4: Computational time comparison.

	Benenson et al.'s protocol	Yuan et al.'s protocol	Yoon et al.'s protocol	Our protocol
Registration phase	$1T_{EXP}$	$4T_H$	$3T_H$	$2T_H$
Login and authentication phases	$2nT_H + 3nT_{EXP}$	$9T_H$	$10T_H$	$4T_{RC5} + 2T_{MAC} + 6T_H$
Total	$2nT_H + 3nT_{EXP} + 1T_{EXP}$	$13T_H$	$13T_H$	$4T_{RC5} + 2T_{MAC} + 8T_H$
Total time	375000 ms*	47.268 ms	47.268 ms	36.368 ms

*Time required for the authentication phase on sensor node only for one session [3].
T_{EXP}: the time required to achieve a modular exponential computation.
n: number of sensors in the communication range of the user.

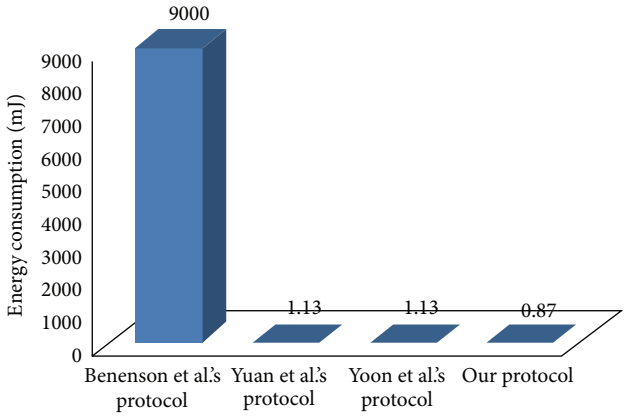

Figure 7: Comparison of energy consumption.

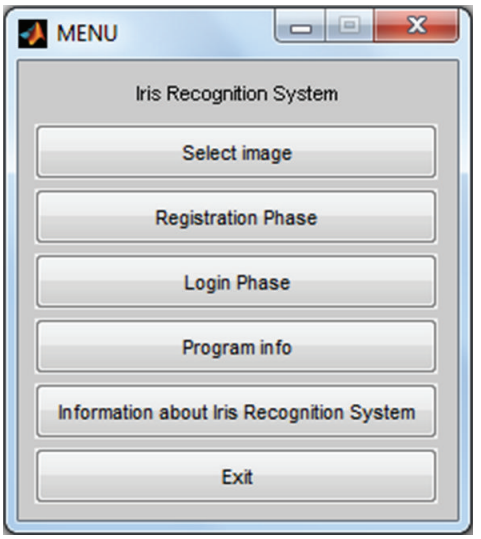

Figure 8: Iris recognition system.

We compute the energy consumption of security computations by (1) to (3) [21]. For Mica2 mote, $I = 8$ mA if the processor status is in active mode. In general, if two new AA batteries are used, $V = 3.0$ V [21]. Therefore, total energy consumption of our protocol is only 0.87 mJ, which is more efficient than Benenson et al.'s protocol (9000 mJ), Yuan et al.'s protocol (1.13 mJ), and Yoon et al.'s protocol (1.13 mJ) as shown in Figure 7:

$$E = V \times Q. \tag{1}$$

Since

$$Q = I \times t, \tag{2}$$

and therefore,

$$E = V \times I \times t, \tag{3}$$

where E denotes the energy consumption, Q is the charge, V is the voltage, I is the current, and t is the elapsed time.

6. Implementation-Based Performance Evaluation

In this section, we introduce the performance evaluation based on the implementation.

6.1. Iris Recognition System. The biometric systems give automatic identifications of the persons derived from a unique characteristics or features. Iris recognition has many advantages such as it has an internal organ (body part), reliable, and does not need to be identified by touching used equipment so iris is considered one of the most important biometric recognition systems.

Our iris recognition system (Figure 8) is performed by Masek's method [22]; some modifications are introduced to Masek's method to achieve the biometric encryption. This iris recognition system uses the global transform to segment the image. Therefore, it can detect the pupil and the iris region. After normalizing the image, the data is extracted and quantized to encode the unique pattern of the iris image using 1D Log-Gabor filters. All tests are performed with CASIA iris image database [23]. Our iris recognition system requires only 4.6570 seconds to extract the features of iris and create BE *template*. For regenerating the user's key, our system requires 4.8280 seconds.

6.2. Simulation-Based Performance Evaluation. In this section, we evaluate the performance of our protocol by MATLAB simulator version R2010a [24]. Results of our simulation comprise not security computational cost only, but also communication cost for transmitting security messages. We will assess the performance of our protocol in the presence of homogeneity and heterogeneity to prove the robustness of

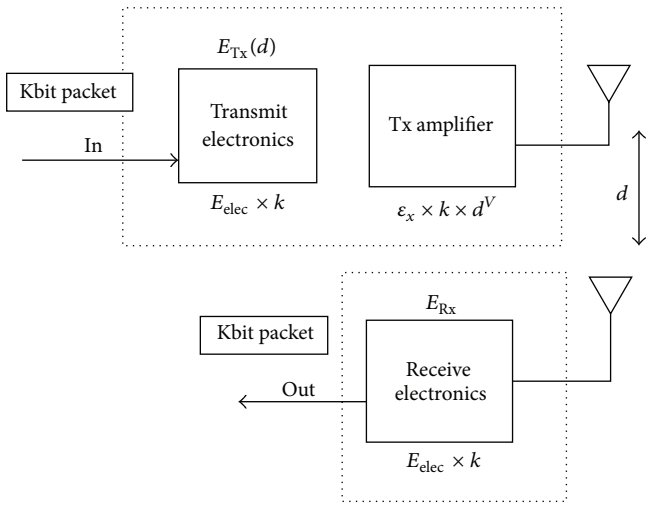

Figure 9: Energy dissipation model.

our protocol, and it works well regardless of network kind. For the aim of this research, we apply similar energy model as discussed in [25, 26] shown in Figure 9.

In this energy model, the energy dissipated per bit (E_{elec}) is 50 nJ/bit for running the receiver or transmitter circuits and the transmit amplifier (ε_{amp}) is 10 pJ/bit/m^2. The energy expended to send k-bits is

$$E_{Tx}(k,d) = E_{Tx\text{-}elec}(k) + E_{Tx\text{-}amp}(k,d),$$
$$E_{Tx}(k,d) = E_{elec} \times k + \varepsilon_{amp} \times k \times d^2, \quad (4)$$

where d is the distance between the sender and the receiver, and E_{Tx} includes the loss of energy because of channel attenuation.

The energy expended to receive k-bits is

$$E_{Rx}(k) = E_{elec} \times k. \quad (5)$$

Also, we assume that the same amount of energy is needed to send k-bits from A to B and vice versa. The parameters used in our simulation are summarized in Table 5.

Security Primitives Choice. Traditional wisdom states select either AES or DES when a block cipher is required. Nevertheless, DES is too slow to be implemented on limited resources devices, and AES is also quite slow. Moreover, AES has the drawback that its block length is long. Skipjack and RC5 are the most appropriate to be implemented on limited resources devices [21]. RC5 has been proven to be secure in the literature [27]. Therefore, we choose RC5 (size of key = 20 byte) as a block cipher. Also, we choose HMAC-SHA1 (size of key = 20 byte) as a MAC function. Value of SHA-1 is 20 bytes.

6.2.1. Homogeneous Wireless Sensor Networks. In this study, we assume that the homogeneous wireless sensor network shown in Figure 10 has the following properties.

(i) Supposing a 120 m × 120 m region of 100 sensors.

Table 5: The parameters used in our simulation.

Parameter	Value
Number of sensor nodes	$n = 100$
Packet size	$k = 4000$ bits
Area	$A = M \times M = 120 \times 120$
GW-node location	(50, 50)
Number of runs	10
MAC protocol	CDMA and TDMA
Communication model	Bi-direction
Transmitter/receiver electronics	$E_{elec} = 50$ nJ/bit
Initial energy for normal node	$E_o = 0.5$ J
Data aggregation energy	$E_{DA} = 5$ nJ/bit/message
Transmit amplifier	$\varepsilon_{amp} = 10$ pJ/bit/m^2

(ii) The sensor nodes are uniformly distributed (i.e., they are randomly distributed in a 2-dimensional space).

(iii) The sensor nodes are static.

(iv) It is supposed that the GW node is placed at the center of the sensing region.

(v) At the network layer, the LEACH (low energy adaptive clustering hierarchy) [25] is used for the routing protocol. Typically, the stability period for LEACH protocol is 995 rounds [28].

The results are present in Figure 11, which compare delay of cases without (w/o) and with (w/) in the proposed protocol and are evaluated during the stability period of network. In the first case (i.e., without the proposed protocol), there were only plain texts transmitted between the accessed node and the user. For the second case (i.e., with the proposed protocol), all security communications and computations of proposed protocol were considered. The communicational and computational cost with the proposed protocol is 99.89 seconds, while without the proposed protocol is 97.37 seconds. This means that the proposed protocol only increases only by 2.59% delay. Briefly, the final results of the simulation demonstrate a small increase of cost of proposed protocol compared with a former case. As a result, such delay is insignificant for the WSN.

Figure 12 shows one that authentication of Benenson et al.'s protocol takes approximately 440 seconds, while one authentication of our protocol takes only 0.53 second. In addition, Benenson et al.'s protocol needs the certificate and public key of a user at the side of receiver, which have been transmitted with each request of user (i.e., rising overhead of transmission). It is clear that the performance of our protocol is high enough compared to that of Benenson et al.'s protocol (by 83574.05%).

6.2.2. Heterogeneous Wireless Sensor Networks. We suppose that heterogeneous wireless sensor network such as Figure 13 has the following properties of heterogeneity.

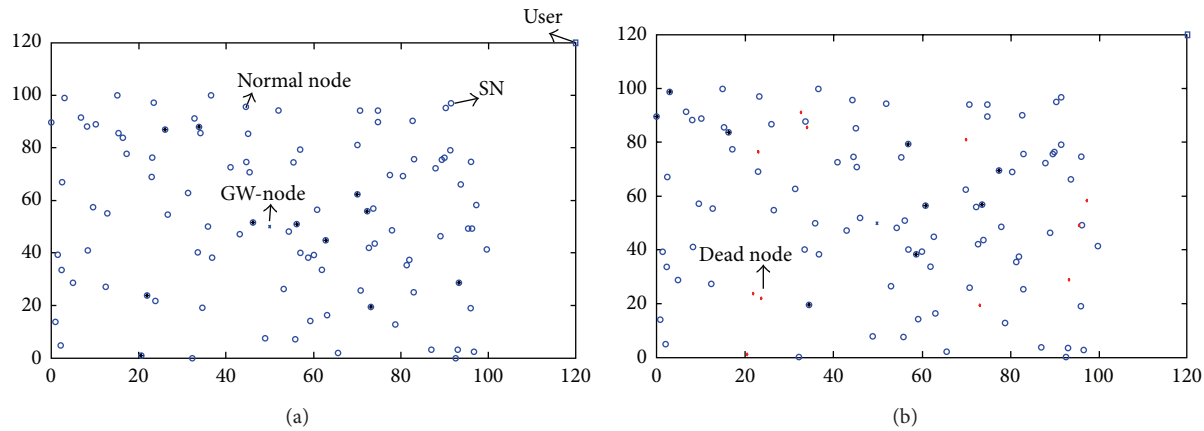

FIGURE 10: (a) A homogeneous wireless sensor network when all the sensor nodes are alive, (b) the network when some sensor nodes are dead.

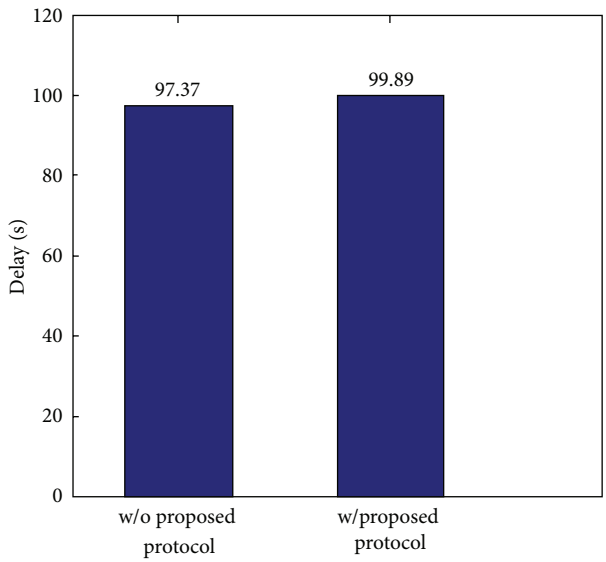

FIGURE 11: Delay performance of homogeneous network.

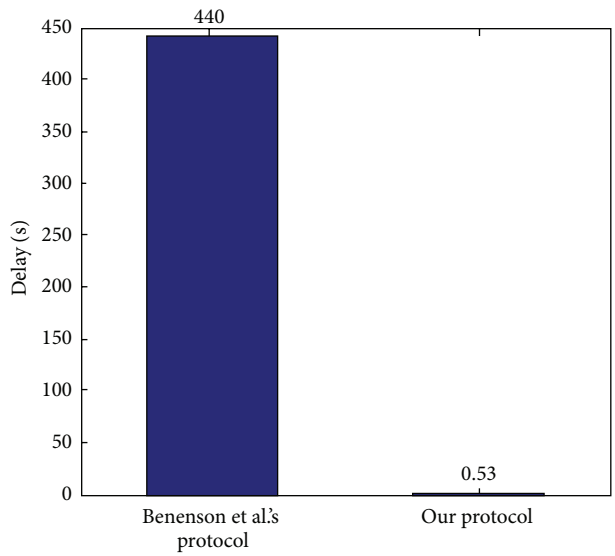

FIGURE 12: Comparison of delay.

(i) The SEP (stable election protocol) [26] is used at the network layer. Typically, the stability period for SEP protocol is 1385 rounds [28].

(ii) The heterogeneity parameters are the fraction of advanced nodes (m = 10%) and the additional energy level between advanced node and normal node (α = 1).

The communicational and computational cost during the stability period of heterogeneous network with the proposed protocol is 137.89 seconds, while without the proposed protocol is 135.24 seconds as explained in Figure 14. This means that the proposed protocol increases only by 1.96% delay. In brief, the final results of the simulation show a small increase of cost of the proposed protocol compared to a normal case. Therefore, our protocol is robustness and works well regardless of network kind.

7. Conclusion and Future Work

In this paper, we have conducted a study on the security of WSNs in the field of authentication. We have studied the existing protocols of user authentication in WSNs. Furthermore, we suggest a biometric-based user authentication protocol. The above analysis proves that our protocol is more practical than the representative protocols and proves the robustness of our protocol since it works well regardless of network kind.

The main advantage of the proposed protocol, which dramatically enhances security aspects in WSNs, is that the user's iris is used to regenerate the user's key on-the-fly every time the user wants be authenticated. In the future, a hardware implementation (with real sensors) of our protocol will be conducted to analyze its real performance and efficiency. Also, we will improve the iris recognition system to introduce

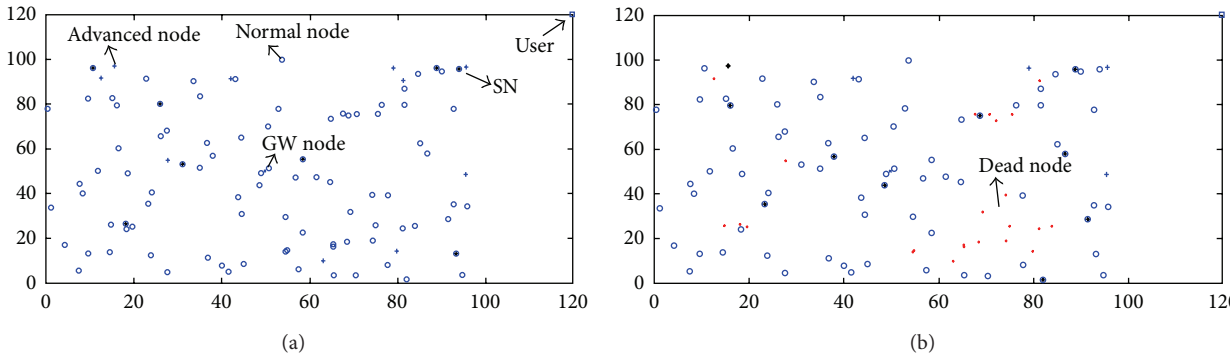

FIGURE 13: (a) A heterogeneous wireless sensor network when all the sensor nodes are alive, (b) the network when some sensor nodes are dead.

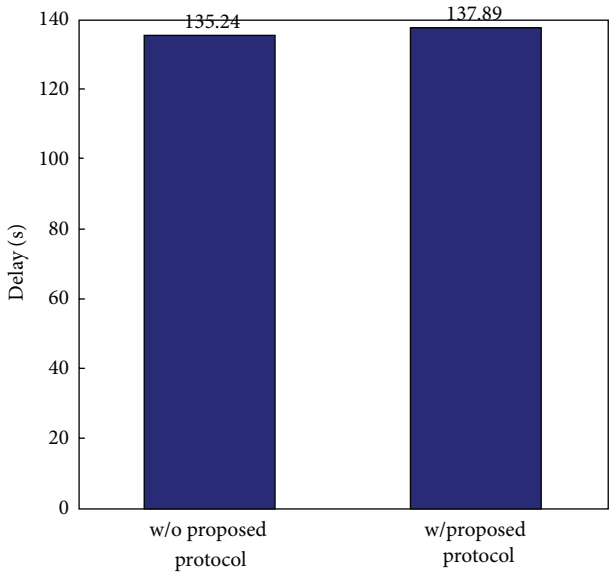

FIGURE 14: Delay performance of heterogeneous network.

detection methods to prevent attacks based on using artificial iris images.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group no. RGP-VPP-264.

References

[1] C.-Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[2] P. Kumar and H.-J. Lee, "Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks," in *Proceedings of the Wireless Advanced (WiAd '11)*, pp. 241–245, London, UK, 2011.

[3] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authentication in sensor networks," in *Real-World Wireless Sensor Networks (REALWSN)*, vol. 14, 2005.

[4] K. H. M. Wong, Z. Yuan, C. Jiannong, and W. Shengwei, "A dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp. 244–251, Taichung, Taiwan, June 2006.

[5] 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, Washington, DC, USA, November 2007.

[6] L.-C. Ko, "A novel dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the IEEE International Symposium on Wireless Communication Systems, ISWCS'08*, pp. 608–612, Reykjavik, Iceland, October 2008.

[7] B. Vaidya, J. J. Rodrigues, and J. H. Park, "User authentication schemes with pseudonymity for ubiquitous sensor network in NGN," *International Journal of Communication Systems*, vol. 23, no. 9-10, pp. 1201–1222, 2010.

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

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

[10] D. H. Nyang and M. K. Lee, "Improvement of Das's two-factor authentication protocol in wireless sensor networks," http://eprint.iacr.org/2009/631.pdf.

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

[12] K. S. Arikumar and K. Thirumoorthy, "Improved user authentication in wireless sensor networks," in *Proceedings of the International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT '11)*, pp. 1010–1015, Tamil Nadu, India, March 2011.

[13] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

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

[15] E.-J. Yoon and K.-Y. Yoo, "A new biometric-based user authentication scheme without using password for wireless sensor

networks," in *Proceedings of the 20th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 279–284, Paris, France, 2011.

[16] S. Mohammadi and S. Abedi, "ECC-based biometric signature: a new approach in electronic banking security," in *Proceedings of the International Symposium on Electronic Commerce and Security (ISECS '08)*, pp. 763–766, Guangzhou City, China, August 2008.

[17] A. Al-Hussain and I. Al-Rassan, "A biometric-based authentication system for web services mobile user," in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM '10)*, pp. 447–452, New York, NY, USA, November 2010.

[18] E. D. Leeuw, *Policies and Research in Identity Management: First IFIP WG11. 6 Working Conference on Policies and Research in Identity Management (IDMAN '07), RSM Erasmus University*, Springer, Rotterdam, The Netherlands, 2008.

[19] 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 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN'04*, pp. 59–64, New York, NY, USA, October 2004.

[20] M. R. Islam, M. S. Sayeed, and A. Samraj, "Biometric template protection using watermarking with hidden password encryption," in *Proceedings of the International Symposium on Information Technology (ITSim '08)*, vol. 1, pp. 1–8, 2008.

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

[22] L. Masek, "Recognition of human irispatterns for biometric identification," The University of Western Australia, http://people.csse.uwa.edu.au/pk/studentprojects/libor/LiborMasekThesis.pdf.

[23] Chinese Academy of Sciences, Institute of Automation, Database of 756 Greyscale Eye Images. Version 1. 0, 2003, http://www.sinobiometrics.com/.

[24] MATLAB simulator, http://www.mathworks.com/products/matlab/.

[25] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Siences (HICSS '33)*, January 2000.

[26] G. Smaragdakis, I. Matta, and A. Bestavros, "SEP: a stable election protocol for clustered heterogeneous wireless sensor networks," Tech. Rep., Boston University Computer Science Department, 2004.

[27] X. H. Le, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," *Journal of Networks*, vol. 6, no. 3, pp. 355–364, 2011.

[28] F. A. Aderohunmu, J. D. Deng, and M. Purvis, "Enhancing clustering in wireless sensor networks with energy heterogeneity," *International Journal of Business Data Communications and Networking*, vol. 7, no. 4, pp. 18–31, 2011.