 CMC, vol.58, no.2, pp.545-565, 2019

A Lightweight Three-Factor User Authentication Protocol for the Information Perception of IoT

Liang Kou[1], Yiqi Shi[2], Liguo Zhang[1], Duo Liu[1, *] and Qing Yang[3]

Abstract: With the development of computer hardware technology and network technology, the Internet of Things as the extension and expansion of traditional computing network has played an increasingly important role in all professions and trades and has had a tremendous impact on people lifestyle. The information perception of the Internet of Things plays a key role as a link between the computer world and the real world. However, there are potential security threats in the Perceptual Layer Network applied for information perception because Perceptual Layer Network consists of a large number of sensor nodes with weak computing power, limited power supply, and open communication links. We proposed a novel lightweight authentication protocol based on password, smart card and biometric identification that achieves mutual authentication among User, GWN and sensor node. Biometric identification can increase the non-repudiation feature that increases security. After security analysis and logical proof, the proposed protocol is proven to have a higher reliability and practicality.

Keywords: Authentication, biometrics, smart card, multi-factor.

1 Introduction

Nowadays, IoT (Internet of Things) is gaining widespread attention from governments, enterprises and academics for several reasons. IoT First of all, the IoT is an important part of the new generation of information technology and plays a catalytic role in social development. Second, the application of the IoT will have enormous economic benefits. According to the estimation of relevant experts, the output value of the IoT will reach one trillion level. The Internet of things is mainly composed of perception layer, transport layer and network layer [Sathishkumar and Patel (2014)]. In this paper, we mainly consider the protection of perception data and regard the wireless sensor networks (WSNs) as the perception layer of the IoT. WSNs are the network that consists of large number of sensor nodes in a self-organized manner. The sensor nodes have the following characteristics, such as limited battery capacity, simple CPU, small storage and communication capability which cause the sensor nodes to suffering from various attacks in hostile environment [Lin, Zhu and Zheng (2017); Wu, Yan, Wang et al. (2017)].

[1] College of Computer Science and Technology, Harbin Engineering University, Harbin, 150001, China.
[2] Harbin University of Commerce, Harbin, 150001, China.
[3] University of North Texas, Denton, 76207, USA.
[*] Corresponding Author: Duo Liu. Email: kevinkl1988@gmail.com.

There are usually two methods for users to access the perceptual data collected by sensor nodes. One is that the user sends query instructions through the WSNs base station or gateway node, and then gets the perceptual data by the corresponding node. The security of this method is guaranteed by the security strategy of WSNs itself and it suffers from large time delay [Das, Sharma and Chatterjee (2012); Qazi (2004)]. The other is that user obtains the real-time data directly from the sensor nodes independent of base station or gateway node. This method has high real-time performance and is suitable for all kinds of real-time applications, but this method needs to consider the legitimacy of the user's identity in particular.

Identity authentication plays a very important role in ensuring that only legitimate users can access resources or services, and key agreement can guarantee that only legitimate communicators can obtain correct communication content. Due to the poor computing power of sensor nodes, traditional security protocols that require large computing power cannot be directly applied in wireless sensor networks. Therefore a lightweight security protocol is needed to secure the WSNs.

The user authentication protocols mainly compose of two-factor user authentication (based on the password and the smart card) and three-factor user authentication (based on two-factor authentication combined with the biometric factor). Practice has proved that three factor biometric-based user authentication is more secure than two-factor user authentication. Biometric identification has the following advantages in the field of user authentication, so it attracts much attention from experts and scholars [Qazi (2004)].

- Biometric identification will not be lost or forgotten;
- Biometric identification is not easy to be replicated;
- Biometric identification is not easy to be forged or distributed;
- Biometric identification is not easy to be guessed.

At present, security solutions to deal with hostile attack in WSNs mostly focus on key management, authentication and secure routing [Balakrishnan and Rino (2016); Amin and Biswas (2015)]. Two-factor authentication [Das, Sharma and Chatterjee (2012); Fan, Ping and Fu (2010); He, Gao and Chan (2010); Khurram and Khaled (2010); Lee, Li and Chen (2011)] combining password and smart card is a common solution for researchers, but two-factor authentication is still not reliable because smart cards are easy to lose and the password is also easily guessed by an attacker. He et al. [He, Kumar and Chilamkurti (2014)] devised a mutual authentication and key agreement scheme based on temporal credential, which can effectively deal with the simulated attacks on user or sensor node, offline password guessing attacks and user anonymous attacks. Their scheme can be put into practical applications in WSNs. However, this solution cannot satisfactorily certify after tracking attacks, insider attacks and identity guessing attacks. In order to solve the above problem, Jiang et al. [Jiang, Ma and Lu (2015)] proposed a linkless enhanced authentication strategy. They took full account of the sensor node's burden and reduced the energy consumption while defending against a series of security threats. Later, They designed a privacy-aware two-factor authentication scheme based on the research results of elliptic curve cryptography (ECC), which took into account the efficiency of WSNs and the safety features in a variety of environments [Jiang, Kumar and Ma (2016)]. Amin et al. [Amin and Biswas (2015)] improved the sensor network architecture and designed a low-energy user authentication and key agreement scheme to achieve two-way authentication, dynamic addition of nodes and password updates, which has improved the session key protection. Choi et al. [Choi, Lee and Kim (2014)] uses a heuristic analysis method and an ECC to improve a user authentication protocol that can reduce the energy consumption of WSNs and provide mutual authentication and key agreement between users and sensors. It can also resist session key attacks and sensor energy exhaustion attacks. In Sahingoz [Sahingoz (2013)], the author presented a key management framework for distributed WSNs that share the keys between sensor nodes and their neighbors. In addition, they used UAV as a management center of asymmetric key to achieve a multi-level dynamic key management. Three-factor user authentication based on biometric [Park and Park (2016)] in the WSNs shows the superior to traditional two-factor user authentication schemes. In this paper, we provide a new user authentication protocol for WSNs using smart card combining with biometric identification. The proposed authentication protocol should achieve these goals: (1) mutual authentication between the user and the sensor node; (2) anonymity: the attacker cannot get the user's identity; (3) session key generation: after the authentication procedure, a session key should be generate shared by the user and the sensor node; (4) GWN does not store the registered user's password and biometric template; (5) attack resistance: the protocol should be robust against a variety of attacks; (6) password update offline. The proposed protocol is lightweight and superior than the exiting protocols on the computational complexity. The security of the proposed protocol is proved by BAN-logic.

The remainder of the paper is organized as follows. In Section 2, we present the related work of user authentication. In Section 3, we review the Althobaiti's protocol and analyze the security vulnerability of Althobaiti's protocol. In Section 4, we describe our proposed new user authentication protocol for WSNs. In Section 5, we perform the security analysis of our scheme by BAN-logic and compare the performance with the existing protocols. In Section 6, we conclude our research.

2 Preliminaries

2.1 Attacker threat model

In order to conduct security analysis of the Althobaiti's protocol and our proposed protocol, we make use of the Dolev-Yao threat model [Ramanujam, Sundararajan and Suresh (2014)] and its improved model [Kim, Lee and Jeon (2014)]. In the unsecured open communications, the attacker has the following abilities:

- An attacker can gain all the messages transmitted over a public channel;
- An attacker can impersonate other communication entities to send messages to users;
- An attacker cannot get correct random number;
- An attacker cannot decrypt the message without the correct key;
- An attacker cannot crack the encryption algorithm;
- Once an attacker steals the user's smart card, he can get all the information stored in the card;

- The ID and password of the user are usually low-entropy;
- An attacker cannot crack the encryption algorithm;
- The gateway node cannot be compromised.

2.2 Fuzzy extractor

Due to the fact that various of noises can lead to the failure of the biometric information acquisition, a fuzzy extractor method [Dodis and Reyzin (2004)] is proposed to extract the correct data with a given error tolerance. A fuzzy extractor method mainly contains two functions: $Gen(\cdot)$ and $Rep(\cdot)$

$Gen(BIO) = (R,P)$

$Rep(BIO') = R$ if BIO is similar to BIO' within a predefined threshold.

The function Gen maps the input biometric information to a secret string $R \in \{0,1\}^l$ and auxiliary information P. The function Rep can reproduce the R with the auxiliary information P and BIO' which is similar to BIO in some degree.

2.3 Notations

The notations used throughout this paper are described in Tab. 1.

Table 1: Notations and parameters

Notation	Description
U_i	User
GWN	Gateway node of WSN
SC	Smart card
BIO_i	Biometric template of U_i
ID_i	Identity of U_i
ID_{sc}	Identity of SC
ID_{GWN}	Identity of GWN
X_{GWN}	Secret key of GWN
Y_j	Secret key only shared by GWN and S_j
PW_i	Password of U_i
sk	Session key

3 Review of Althobaiti's protocol

In this section, we review Althobaiti et al.' user authentication protocol [Moreover and Section (2013)]. The notations used in the paper are listed in Tab. 1. Althobaiti's protocol takes advantage of the biometric identification to enhance security and it includes three processes: registration phase, login phase and authentication phase.

3.1 Registration phase

When the new user U_i wants to access the perceptual data collected by the sensor node S_j, he needs to register to the GWN firstly. The Registration Phase of user U_i includes the following procedures:

- The GWN selects and saves a random key ek_i for the new user U_i;
- The user U_i inputs his identity identification ID_i and biometric information BIO_i. Then computes $BE = h(B_i) \oplus ek_i$ and stores BE in the device of U_i;
- The GWN calculates $F_i = h(ID_i \oplus X)$, and send the message $\{ID_i, F_i\}$ to the U_i via secure channel;
- The U_i stores the data $\{ID_i, F_i, h(ek_i), BE\}$.

3.2 Login phase

The login phase of user U_i includes the following procedures:

- The user U_i inputs ID_i and BIO_i and calculates $N = h(B_i)$, $ek_i' = BE \oplus h(B_i)$;
- U_i calculates $h(ek_i')$ and verifies if $h(ek_i') = h(ek_i)$. If yes, U_i sends the login request message $\{ID_i, request\}$ to GWN. If no, it terminates the operation.

3.3 Authentication phase

The authentication phase realizes mutual authentication between user U_i and sensor node S_j. A detailed description of this phase is as follows:

- After GWN receives the message $\{ID_i, request\}$, GWN sends a authentication request $\{R\}$ where R selected randomly to U_i as the login response. After U_i receives $\{R\}$, U_i performs the encryption $\{R, T_1\} \rightarrow E_{eki}\{R, T_1\}$ based on the key ek_i, where T_1 represents the timestamp of U_i. U_i sends the authentication request message $E_{eki}\{R, T_1\}$ to GWN via public channel.
- GWN receives the message $E_{eki}\{R, T_1\}$ at T_2 and decrypts the message to acquire the $D_{eki}\{R, T_1\}$ according to ek_i. Then GWN verifies if $|T_1 - T_2| \le \Delta T$. If no, it terminates the operation. If yes, sensor node S_j responses to U_i.
- GWN calculates

$$F_i = h(ID_i \oplus X)$$

$$Y_i = MAC_{F_i}(ID_i \| ID_j \| T_3)$$

where, T_3 represents the current timestamp of GWN. GWN sends the message $\{ID_i, Y_i, T_3\}$ via public channel.

- S_j receives the message $\{ID_i, Y_i, T_3\}$ at T_4. S_j verifies if $|T_4 - T_3| \le \Delta T$. If no, it terminates the operation. If yes, it calculates the following equations:

$$F_i = h(ID_i \oplus X)$$

$$Y_i' = MAC_{F_i}(ID_i \| ID_j \| T_3)$$

S_j verifies if Y_i' equals to Y_i. If no, it terminates the operation. If yes, S_j responses to U_i with RM and computes the following equations:

$$V_i = h(ID_i \| F_i \| T_5)$$

$$C_i = h(RM)$$

$$L = E_{V_i}(RM, C_i)$$

S_j sends the message $\{L, T_5\}$ to U_i via public channel, where T_5 represents the current timestamp of S_j.

- U_i receives the message $\{L, T_5\}$ at T_6 and verifies if $|T_6 - T_5| \le \Delta T$. If no, U_i terminates the operation. If yes, U_i computes the following equations:

$$V_i = h(ID_i \| F_i \| T_5)$$

$$D_{V_i}(L) = (RM', C_2')$$

$$C_i^* = h(RM')$$

If $C_i^* = C_I'$, U_i accepts the RM as the legal request response, else U_i rejects the RM, where $V_i = h(ID_i \| F_i \| T_5)$ is regarded as the session key between U_i and S_j.

4 Security analysis of Althobaiti's protocol

Althobaiti's protocol is a typical light-weight user authentication protocol based on biometric identification. It reduces computational complexity effectively because it only applies hash function, XOR operation, concatenation operation and symmetric encryption without complex asymmetric encryption. It can resist attacks such as stolen smart card attack and stolen verifier attack. However, Althobaiti's protocol is only based on biometric identification that has some Security Flaws. We utilize the Dolev-Yao attacker expansion model to analyze the security flaws existing in the Althobaiti's protocol.

4.1 Node compromise attack

Assume that an attacker A first captures a sensor node S_j, then obtains secret key X. The attacker A intercepts messages $\{ID_i, Y_i, T_3\}$ and $\{L, T_5\}$ then A calculates the following formulas:

$$F_i = h(ID_i \oplus X)$$

$$V_i = h(ID_i \| F_i \| T_5)$$

A can may get the correct value V_i by constantly trying different T_5, where V_i is the session key shared by U_i and S_j. A can steal the session key through the following steps:

Step one: GWN send messages $\{ID_i, Y_i', T_3'\}$ and $\{L', T_5'\}$ to S_j' in the Authentication Phase, where

$$F_i = h(ID_i \oplus X)$$

$$Y_i' = MAC_{F_i}(ID_i \| ID_j' \| T_3')$$

$$V_i' = h(ID_i \| F_i \| T_5')$$

$$C_i' = h(RM)$$

$$L' = E_{V_i}(RM, C_i')$$

Step two: A intercepts messages $\{ID_i, Y_i', T_3'\}$ and $\{L', T_5'\}$ and obtains the parameters X, ID_i and T_5', then calculates $V_i' = h(ID_i \| F_i \| T_5')$, so A acquires the session key between U_i and S_j. When A successfully compromises a node, he can obtain session keys for all nodes. So this protocol cannot resist the node compromise attack.

4.2 *GWN* impersonation attack

We can prove that an attacker A can impersonate the GWN to authenticate sensor node. The detail steps are as follows.

Step one: A captures the sensor node S_j, gets the secret key X, and intercepts the message $\{ID_i, Y_i, T_3\}$ in the authentication phase.

Step two: A calculates the follow formulas:

$$F_i' = h(ID_i \oplus X)$$

$$Y_i' = MAC_{F_i}(ID_i \| ID_j' \| T_3')$$

where, ID'_j represents the ID of sensor node S_j' queried by U_i, T_3' represents the current timestamp of A. A sends the message $\{ID_i, Y_i', T_3'\}$ to S_j' via the public channel.

Step three: After S_j' receives the message $\{ID_i, Y_i', T_3'\}$, he verifies the freshness of T_3'. If it fails to meet the requirement, the operation is terminated. Else S_j' calculates the following formulas:

$$F_i' = h(ID_i \oplus X)$$

$$Y_i{*} = MAC_{F_i'}(ID_i \| ID_j' \| T_3')$$

If $Y_i^* = Y_i'$, S_j' response to U_i with RM' and computes the following formulas:

$$V_i' = h(ID_i \| F_i \| T_5')$$

$$C_i' = h(RM')$$

$L' = E_{V_i'}(RM', C_i')$

where, T_5' represents the current timestamp of S_j'. S_j' sends the message $\{L', T_5'\}$ to U_i .Because the attacker can calculate the session key V_i' through X, ID_i and T_5', the protocol cannot resist the GWN impersonation attack.

4.3 Man-in-the-middle attack

An attacker can implement the Man-in-the-middle attack through the following processes:

Step one: A captures node S_j, obtains the secret key X, and intercepts the message $\{ID_i, Y_i, T_3\}$.

Step two: A calculates the following equations:

$F_i^* = h(ID_i \oplus X)$

$Y_i^* = MAC_{F_i^*}(ID_i \| ID_j \| T_3^*)$,

where T_3^* represents the current timestamp of A. A modifies message $\{ID_i, Y_i^*, T_3^*\}$

Step three: After S_j receives message $\{ID_i, Y_i^*, T_3^*\}$, it verifies the freshness of the T_3^*, and computes the following equations:

$F_i = h(ID_i \oplus X)$

$Y_i^{**} = MAC_{F_i}(ID_i \| ID_j \| T_3^*)$,

S_j verifies if $Y_i^{**} = Y_i^*$. If yes, S_j responses to U_i with RM^* and computes the following equations:

$V_i^* = h(ID_i \| F_i \| T_5^*)$

$C_i^* = h(RM^*)$

$L^* = E_{V_i^*}(RM^*, C_i^*)$

S_j the message $\{L^*, T_5^*\}$ to U_i.

Step four: A intercepts message $\{L^*, T_5^*\}$ and computes $V_i^{**} = h(ID_i \| F_i^* \| T_5^*)$. A decrypts L^* to obtain RM^*, C^*. Besides, A can create response message RM^{**} to replace RM^*, and calculates:

$C_i^{**} = h(RM^{**})$

$L^{**} = E_{V_i^{**}}(RM^{**}, C_i^{**})$

Finally, A sends the message $\{L^{**}, T_5^*\}$ to U_i. U_i will authenticate $\{L^{**}, T_5^*\}$ successfully and regard RM^{**} as the legal response, so the protocol cannot resist the Man-in-the-middle attack.

4.4 Privileged-insider attack

In the Registration Phase *GWN* randomly generates ek_i for U_i and stores ek_i in the database. Privileged-insider attack can obtain the ek_i to decrypt message $E_{eki}\{R,T_1\}$ and forge a faked U_i . So the protocol cannot resist the Privileged-insider attack.

5 The proposed user authentication protocol

In order to improve the existing security flaws of Althobaiti's protocol, we propose a novel user authentication protocol based on biometric identification combined with smart card and password. The proposed protocol includes registration phase, login phase, authentication phase, and biometric identity update phase.

5.1 Registration phase

In this phase, U_i register with *GWN* . Fig. 1 illustrates the registration phase and it is performed as follows.

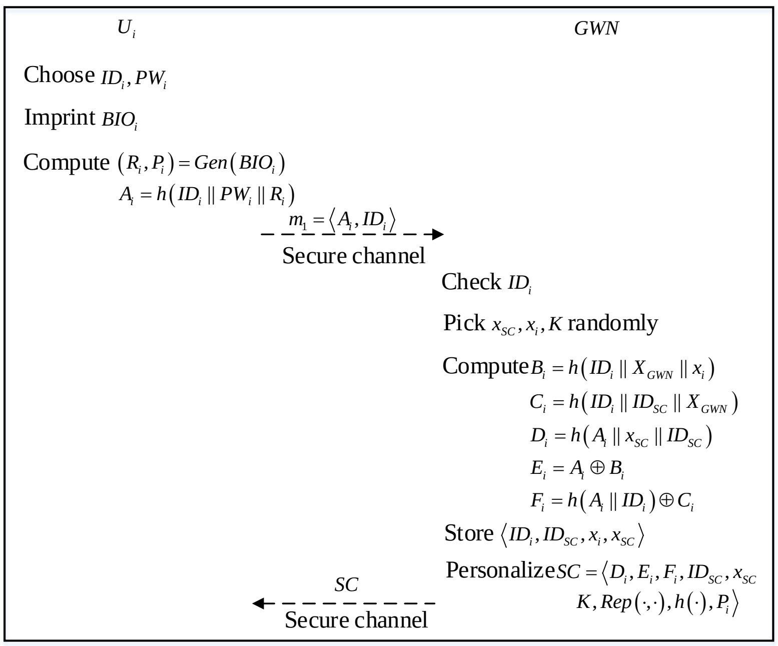

Figure 1: Registration phase

- Step 1: U_i chooses ID_i , PW_i , and imprints biometric BIO_i , and computes $(R_i, P_i) = Gen(BIO_i)$ and $A_i = h(ID_i, PW_i, R_i)$. Then sends $m_1 = \langle A_i, ID_i \rangle$ to *GWN* via a secure channel.
- Step 2: *GWN* checks if ID_i exists in the database, if no, U_i is recommended to select a new identity; otherwise, *GWN* picks x_{SC} , x_i and K randomly, and computes $B_i = h(ID_i, X_{GWN}, x_i)$

$$C_i = h\left(ID_i, ID_{SC}, X_{GWN}\right),$$
$$D_i = h\left(A_i, x_{SC}, ID_{SC}\right),$$
$$E_i = A_i \oplus B_i,$$
$$F_i = h\left(A_i, ID_i\right) \oplus C_i.$$

- Step 3: the parameters $\langle ID_i, ID_{SC}, x_i, x_{SC} \rangle$ are stored by GWN. GWN issues the smart card $SC = \langle D_i, E_i, F_i, ID_{SC}, x_{SC}, K, Rep(\cdot,\cdot), h(\cdot), P_i \rangle$ and sends the smart card to U_i via a secure channel.

5.2 Login phase

When U_i wants to access the node S_j, the login request is launched at first by U_i with SC. Fig. 2 illustrates the login phase and it is performed as follows.

U_i GWN

Enter ID_i, PW_i, BIO_i

Compute $R_i^{'} = Rep\left(BIO_i, P_i\right)$

$A_i^{'} = h\left(ID_i^{'} \| PW_i^{'} \| R_i^{'}\right)$

Check $h\left(A_i^{'} \| x_{SC} \| ID_{SC}\right) \stackrel{?}{=} D_i$

Pick N_i, n_1 randomly

Compute $B_i^{'} = A_i \oplus E_i$

$C_i^{'} = h\left(A_i^{'} \| ID_i\right) \oplus F_i$

$UV_1 = E_K\left(ID_i \| ID_{SC} \| N_i\right)$

$VC_1 = h\left(B'_i \| C'_i \| N_i \| n_1\right)$

Choose ID_j

Compute $UV_2 = ID_j \oplus h\left(ID_i \| N_i \| n_1\right)$

$m_2 = \langle ID_i, UV_1, UV_2, VC_1, n_1 \rangle$ →

Figure 2: Login phase

- Step 1: U_i inserts SC and enters ID_i, PW_i and imprint BIO_i.
- Step 2: SC computes $R_i' = Rep(BIO_i, P_i)$, $A_i' = h(ID_i, PW_i, R_i')$ and checks whether $h(A_i', x_{SC}, ID_{SC})$ equals to D_i. If yes, SC picks two random number N_i and n_i, and computes

$$B_i' = A_i \oplus E_i,$$
$$C_i' = h(A_i', ID_i) \oplus E_i,$$
$$UV_1 = Ek(ID_i, ID_{SC}, N_i),$$
$$VC_1 = h(B_i', C_i', N_i, n_1),$$

$UV_2 = ID_j \oplus h(ID_i, N_i, n_1)$

- Step 3: SC sends $m_2 = \langle ID_i, UV_1, UV_2, VC_1, n_1 \rangle$ to GWN, where n_1 is a random number.

5.3 Authentication phase

Fig. 3 illustrates the authentication phase and it is performed as follows.

- Step 1: GWN checks the validity of ID_i and the freshness of n_1. If yes, it computes $(ID_i, ID_{SC}, N_i) = D_k(UV_1)$, $C_i = h(ID_i, ID_{SC}, X_{GWN})$, and $B_i = h(ID_i, X_{GWN}, x_i)$, and checks whether $h(B_i, C_i, N_i, n_1)$ equals to VC_1. If yes, GWN computes $ID_j = UV_2 \oplus h(ID_i, N_i, n_1)$,

$Y_j = h(ID_j, X_{GWN})$,

$VC_2 = h(ID_i, ID_j, ID_{GWN}, Y_j, N_i, n_2)$,

$GV_1 = ID_i \oplus h(ID_{GWN}, Y_j, N_i)$,

$GV_2 = N_i \oplus h(ID_i, ID_j, Y_j)$.

GWN sends $m_3 = \langle ID_i, ID_{GWN}, GV_1, GV_2, VC_2, n_2 \rangle$ to S_j, where n_2 is a random number.

- Step 2: S_j checks the freshness of n_2. If n_2 meets freshness requirement, S_j computes

$ID_j = GV_1 \oplus h(ID_{GWN}, Y_j, N_i)$,

$N_j = GV_2 \oplus h(ID_i, ID_j, Y_j)$.

Then, it checks whether $h(ID_i, ID_j, ID_{GWN}, Y_j, N_i, n_2)$ equals to VC_2. Next, S_j picks N_j and n_3 randomly and computes

$sk_s = h(ID_i, ID_j, N_i, N_j)$

$VC_3 = h(sk_s, Y_j, N_i, N_j, n_3)$

$SG = h(ID_i, ID_j, Y_j) \oplus N_j$.

After that, S_j sends $m_4 = \langle VC_3, SG, n_3 \rangle$ to GWN, where n_3 is a random number.

- Step 3: GWN checks the freshness of n_3. If n_3 meets the freshness requirement, GWN computes:

$N_j = SG \oplus h(ID_i, ID_j, Y_j)$,

$sk_g = h(ID_i, ID_j, N_i, N_j)$.

Then GWN checks whether $h(sk_g, Y_j, N_i, N_j, n_3)$ equals to VC_3. If yes, GWN computes:

$VC_4 = h(sk_g, B_i, C_i, ID_i, ID_j, N_j, n_4)$,

$GU = E_k(N_i, N_j)$.

After that, GWN sends $m_5 = \langle VC_4, GU, n_4 \rangle$ to U_i, where n_4 is a random number.

- Step 4: U_i checks the freshness of n_4. If n_4 meets freshness requirement, U_i computes:

$(N_i, N_j) = D_k(GU)$,

$sk_u = h(ID_i, ID_j, N_i, N_j)$.

Then he checks whether $h(sk_u, B_i, C_i, ID_i, ID_j, N_j, n_4)$ equals to VC_4. If yes, U_i accepts GWN and S_j, and agree the session key $sk_u = sk_s = sk$.

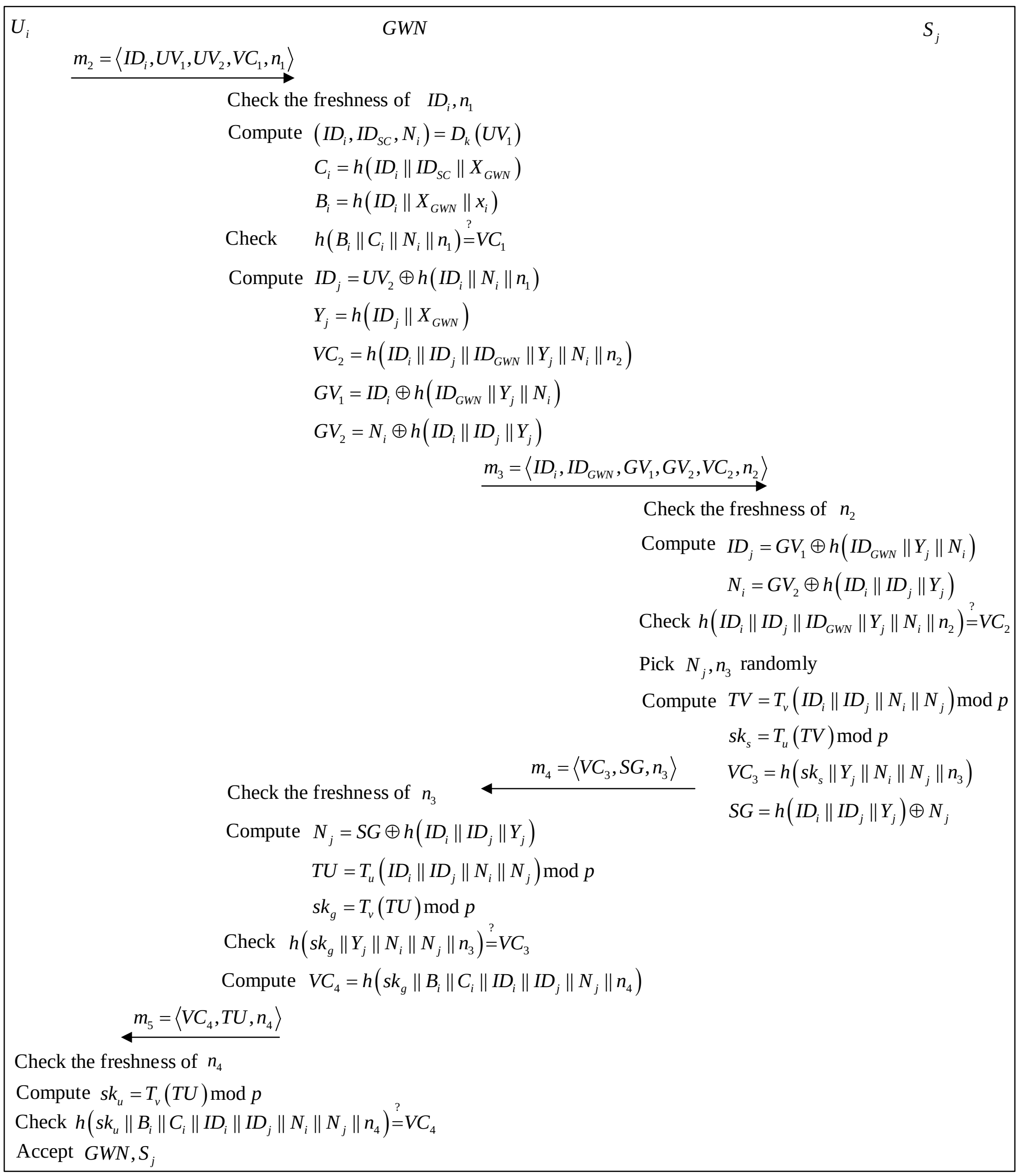

Figure 3: Authentication phase

5.4 Update phase

A legal user can update the old password PW_i and the biometric BIO_i as follows:

- Step 1: U_i inserts the smart card SC into a card reader, then U_i inputs the ID_i, old password PW_i and imprints old biometric BIO_i.
- Step 2: SC computes $R_i = Rep(BIO_i, P_i)$, $A_i = h(ID_i, PW_i, R_i)$, and checks whether $h(A_i, x_{SC}, ID_{SC})$ equals to SC. If yes, D_i computes:

$B_i = A_i \oplus E_i$,

$C_i = h(A_i, ID_i) \oplus F_i$,

U_i inputs new PW_i and imprints new biometric BIO_i.

- Step 3: SC computes:

$R_i' = Rep(BIO_i', P_i)$,

$A_i' = h(ID_i, PW_i', R_i')$,

$D_i' = h(A_i', x_{SC}, ID_{SC})$,

$E_i' = A_i' \oplus B_i$,

$F_i' = h(A_i', ID_i) \oplus C_i$.

- Step 4: The smart card updates the parameter to $SC = \langle D_i', E_i', F_i', ID_{SC}, x_{SC}, K, Rep(\cdot,\cdot), h(\cdot), P_i \rangle$ without GWN.

6 Security analysis and performance comparison

6.1 Proof of authentication and key agreement based on BAN Logic

6.1.1 The BAN logic postulates

Table 2: Notations and parameters of ban logic

Notation	Meaning
$P\mid\equiv X$	P believes X
$\#(X)$	X is freshness
$P \Rightarrow X$	P has jurisdiction over X
$P \lhd X$	P sees X, or P once received X
$P\mid\sim X$	P once said X, or P once forward X
(X, Y)	X or Y is part of formula (X, Y)
$\langle X\rangle_Y$	X is combined with Y
$\{X\}_Y$	encrypt X using Y
$P \overset{K}{\leftrightarrow} Q$	only P and Q share key K
$P\mid\equiv X$	P believes X
$\#(X)$	X is freshness

(1) Message meaning rule of shared key

$$\frac{P \mid\equiv P \overset{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \mid\equiv Q \sim X}$$

(2) Nonce verification rule

$$\frac{P \mid\equiv \#(X), P \mid\equiv Q \sim X}{P \mid\equiv Q \mid\equiv X}$$

(3) Jurisdiction rule

$$\frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

(4) Freshness-conjunction rule

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$$

6.1.2 Security goal

$G_1 : U_i \mid\equiv U_i \overset{sk}{\leftrightarrow} S_j$

$G_2 : S_j \mid\equiv U_i \overset{sk}{\leftrightarrow} S_j$

$G_3 : U_i \mid\equiv S_j \mid\equiv U_i \overset{sk}{\leftrightarrow} S_j$

$G_4 : S_j \mid\equiv U_i \mid\equiv U_i \overset{sk}{\leftrightarrow} S_j$

6.1.3 Idealized form

Message m_2

$U_i \to GWN : (N_i, n_1, ID_i, ID_j, B_i, C_i)_k$

Message m_3

$GWN \to S_j : (N_i, n_2, ID_i, ID_j, ID_{GWN})_{Y_j}$

Message m_4 *:*

$S_j \to GWN : (N_i, N_j, n_3, ID_i, ID_j, sk)_{Y_j}$

Message m_5 *:*

$GWN \to U_i : (N_i, N_j, n_4, ID_i, ID_j, sk, B_i, C_i)_K$

6.1.4 Assumptions

We make the assumptions about the initial state of the scheme to analyze the proposed scheme as follows.

$A_1 : GWN \mid\equiv \#(n_1)$

$A_2 : S_j \mid\equiv \#(n_2)$

$A_3 : GWN \mid\equiv \#(n_3)$

$A_4 : U_i \mid\equiv \#(n_4)$

$A_5 : U_i \mid\equiv U_i \overset{K}{\leftrightarrow} GWN$

$A_6 : GWN \mid\equiv U_i \overset{K}{\leftrightarrow} GWN$

$A_7 : S_j \mid\equiv S_j \overset{y_j}{\leftrightarrow} GWN$

$A_8 : GWN \mid\equiv S_j \overset{y_j}{\leftrightarrow} GWN$

$A_9 : U_i \mid\equiv S_j \Rightarrow U_i \overset{sk}{\leftrightarrow} S_j$

$A_{10} : S_j \mid\equiv U_i \Rightarrow U_i \overset{sk}{\leftrightarrow} S_j$

6.1.5 Security analysis of the idealized form of the proposed scheme

According to m_2, we can easily obtain

$P_1 : GWN \triangleleft (N_i, n_1, ID_i, ID_j, B_i, C_i)_K$

According to A_6 and the message-meaning rule, we have

$P_2 : GWN \mid\equiv U_i \sim (N_i, n_1, ID_i, ID_j, B_i, C_i)$

According to A_1 and the freshness-conjunction rule, we have

$P_3 : GWN \mid\equiv \#(N_i, n_1, ID_i, ID_j, B_i, C_i)$

According to P_2, P_3 and the non-verification rule, we have

$P_4 : GWN \mid\equiv U_i \mid\equiv (N_i, n_1, ID_i, ID_j, B_i, C_i)$

According to m_3, we have

$P_5 : S_j \triangleleft (N_i, n_2, ID_i, ID_j, ID_{GWN})_{Y_j}$

According to A_7 and the message-meaning rule, we have

$P_6 : S_j \mid\equiv GWN \mid\sim (N_i, n_2, ID_i, ID_j, ID_{GWN})$

According to A_2 and the freshness-conjunction rule, we have

$P_7 : S_j \mid\equiv \#(N_i, n_2, ID_i, ID_j, ID_{GWN})$

Then from P_6, P_7 and the non-verification rule, we have

$P_8 : S_j \mid\equiv GWN \mid\equiv (N_i, n_2, ID_i, ID_j, ID_{GWN})$

According to m_4, we have

$P_9 : GWN \triangleleft (N_i, N_j, n_3, ID_i, ID_j, sk)_{Y_j}$

According to A_8 and the message-meaning rule, we have

$P_{10} : GWN \mid\equiv S_j \mid\sim (N_i, N_j, n_3, ID_i, ID_j, sk)$

According to A_3 and freshness-conjunction rule, we have

$P_{11} : GWN \mid\equiv \#(N_i, N_j, n_3, ID_i, ID_j, sk)$

Then according to P_{10}, P_{11} and the non-verification rule, we have

$P_{12}: GWN \mid\equiv S_j \mid\equiv (N_i, N_j, n_3, ID_i, ID_j, sk)$

According to m_5, we have

$P_{13}: U_i \triangleleft (N_i, N_j, n_4, ID_i, ID_j, sk, B_i, C_i)_K$

According to A_4 and the message-meaning rule, we have

$P_{14}: U_i \mid\equiv GWN \mid\sim (N_i, N_j, n_4, ID_i, ID_j, sk, B_i, C_i)$

According to A_5 and freshness-conjunction rule, we have

$P_{15}: U_i \mid\equiv \#(N_i, N_j, n_4, ID_i, ID_j, sk, B_i, C_i)$

Then, from P_{14}, P_{15} and the non-verification rule, we have

$P_{16}: U_i \mid\equiv GWN \mid\equiv (N_i, N_j, n_4, ID_i, ID_j, sk, B_i, C_i)$

Because $sk = h(ID_i, ID_j, N_i, N_j)$ according to P_{16} and P_{12}, we have

$P_{17}: U_i \mid\equiv S_j \mid\equiv U_i \overset{sk}{\leftrightarrow} S_j (G_3)$

Likewise, according to P_4 and P_8, we have

$P_{18}: S_j \mid\equiv U_i \mid\equiv U_i \overset{sk}{\leftrightarrow} S_j (G_4)$

According to P_9, P_{17} and jurisdiction rule, we have

$P_{19}: U_i \mid\equiv U_i \overset{sk}{\leftrightarrow} S_j (G_1)$

Likewise, according to P_{10}, P_{18} and jurisdiction rule, we have

$P_{20}: S_j \mid\equiv U_i \overset{sk}{\leftrightarrow} S_j (G_2)$

According to G_1, G_2, G_3 and G_4, we conclude that both U_i and S_j believe they share the session key users identity, password, SC and biometrics. It can be concluded that our proposed scheme not only provides mutual authentication between user, sensor node and GWN, but also generates a shared session key for subsequent communication.

6.2 Security aalysis against vrious atacks

● **Node capture attack:** Assume that an adversary A physically captures a sensor node S_j, he can access real-time perception data collected by S_j. What is more, A can obtain the secret information including node key and session key sk. Due to the fact that sk is generated by the N_i and N_j corresponding to U_i and S_j, so the session key is different from each other because both the User and Sensor Node are different. One compromising node cannot reveal the information of other nodes and users. Legal users can still communicate with other nodes securely. The proposed protocol can resist Node capture attack.

● **Off-line password guessing attack:** Assume that an adversary A may attempt to guess the password PW_i. He can obtain A_i A_i successfully, if he steal the data from the smart card. He can obtain PW_i successfully only if he knows R_i which is very relevant to the biometric identification BIO_i. BIO_i cannot be forged because of its uniqueness. It is impracticable to guess the password PW_i correctly in our protocol.

- **Smart card loss attack:** Assume that the smart card of a legal user is stolen by an adversary A, and he wants to carry out Smart card loss attack. A can get the information $\langle D_i, E_i, F_i, ID_{SC}, x_{SC}, K, Rep(\cdot,\cdot), h(\cdot), P_i \rangle$ stored in the smart card. Although A can obtain A_i by $D_i = h(A_i, x_{SC}, ID_{SC})$ and $A_i = h(ID_i, PW_i, R_i)$, he cannot obtain PW_i due to the one-way function and R_i without biometric identification BIO_i. The proposed protocol can resist Offline password guessing attack.
- ***GWN* impersonation attack:** Assume that an attacker A physically captures a sensor node S_j and impersonates GWN to attack sensor node SN_j'. In order to be authenticated by the sensor node SN_j', A needs to forge message m_3. Though A can obtain y_j because he captures S_j, he cannot calculate y_j' response to SN_j'. y_j' is the key factors for generating GV_1, GV_2 and VC_2, so A cannot forge message legal m_3. The proposed protocol can resist GWN impersonation attack.
- **Man-in-the-middle attack and replay attack:** Assume that an adversary A can intercept legitimate login request message $m_2 = \langle ID_i, UV_1, UV_2, VC_1, n_1 \rangle$. Due to the feature of one-way hash function, A cannot obtain the key K, the random number N_i, password PW_i and biometric identification value R_i related U_i, so A cannot forge message m_2. What's more, the login request message m_2 is related to n_1 varying with time, so the intercepted m_2 will be invalid over time. Therefore, our protocol can withstands Man-in-the-middle attack and Replay attack.
- **Denial of Service Attack:** In the proposed protocol, U_i, S_j and GWN verify the freshness of fresh factors n_1, n_2, n_3 and n_4 during the authentication process, respectively. Each message for verification such as m_2, m_3, m_4 and m_5 contains a fresh factor. In addition, each of U_i, S_j and GWN verifies if the received value is equal to the recalculated value. The proposed protocol can resist denial of service attack.
- **Mutual Authentication:** The proposed protocol achieve the mutual authentication of each entities U_i, S_j and GWN. GWN authenticates U_i by verifying the validity of m_2 generated by U_i. Then S_j and GWN conduct two-way authentication by checking the validity of m_3 generated by GWN and m_4 generated by S_j. The authentication between U_i and S_j is proved by m_5 generated by GWN. All the legal messages are only produced by legal U_i, S_j and GWN. Therefore, our protocol provides proper mutual authentication.

Tab. 3 shows the security features supported by our protocol and existing protocols [Kim (2014); Chang, Lee, Lin et al. (2015); Yoon and Yoo (2014)]. It is clear to see that our protocol has superiority on the extra important security features compared with existing protocols. We note that the protocol of Kim et al. [Kim (2014); Chang, Lee, Lin et al. (2015); Yoon and Yoo (2014)] is susceptible to several attacks, such as man-in-the-middle attack and impersonation attack. The protocol of Chang et al. [Chang, Lee, Lin et al. (2015)] is prone to man-in-the-middle attack and unauthorized access attack. The protocol of Yoon et al. [Yoon and Yoo (2014)] cannot provide user anonymity which may lead to the privacy information disclosure. Our protocol provides the formal BAN-logic to prove security. Due to biometrics application, our protocol can offer non-repudiation which is regarded as a practical application.

Table 3: Anti-attack performance

	Kim, Lee and Jeon (2014)	[Chang, Lee, Lin et al. (2015)]	[Yoon and Yoo (2014)]	Ours
Password guessing attack	√	√	√	√
User impersonation attack	×	×	√	√
Lost smart card attack	√	×	√	√
Stolen verifier attack	×	√	√	√
Man-in-the-middle attack	√	√	√	√
Replay attack	√	√	√	√
Insider attack	√	√	√	√
Denial of service attack	√	√	√	√
Usage of biometrics	√	√	√	√
Provides user anonymity	×	×	×	√
Usage of ECC	√	√	×	×

6.3 Performance comparisons

Tab. 4 shows the computational load imposed by the authentication protocol in the registration, login, and authentication phases. We denote T_h, T_x, T_F and T_E as one-way hashing operation, XOR operation, fuzzy extractor operation($Gen(\cdot)$ or $Rep(\cdot)$) and symmetric-key encryption or symmetric-key decryption operation ,respectively. In order to reduce computational load, we only use one-way hashing operation and XOR operation to authenticate sensor node. So our protocol is ideal for resource-constrained WSNs.

Table 4: Computational Load Comparison

Scheme		Computation Cost		
		Registration	Login & Authentication	Total
Kim, Lee and Jeon (2014)	User	$2T_h + T_x$	$9T_h + 9T_x$	$11T_h + 10T_x$
	GWN	$6T_h + 3T_x$	$8T_h + 8T_x$	$14T_h + 11T_x$
	Sensor	0	$2T_h + 2T_x$	$2T_h + 2T_x$
Chang, Lee, Lin et al. (2015)	User	$2T_h + T_x$	$9T_h + 5T_x$	$11T_h + 6T_x$
	GWN	$5T_h + 3T_x$	$10T_h + 4T_x$	$15T_h + 7T_x$
	Sensor	0	$4T_h + T_x$	$4T_h + T_x$
Yoon and Yoo (2014)	User	T_h	$3T_h + 2T_x + 2T_E$	$4T_h + 2T_x + 2T_E$
	GWN	$2T_h + 2T_x$	$4T_h$	$6T_h + 2T_x$
	Sensor	0	$3T_h + 2T_E$	$3T_h + 2T_E$
Ours	User	$T_h + T_F$	$7T_h + T_F + 2T_E + 3T_x$	$8T_h + 2T_F + 2T_E + 3T_x$
	GWN	$2T_x + 4T_h$	$2T_E + 4T_x + 12T_h$	$2T_E + 6T_x + 16T_h$
	Sensor	0	$3T_x + 6T_h$	$3T_x + 6T_h$

7 Conclusion

Before introducing our protocol, we review the Althobaiti et al. protocol and analyze its security vulnerabilities. Then we propose a novel three-factor user authentication protocol for the information perception of IoT. The proposed protocol can achieve fast authentication process without biometric templates. It not only effectively solves the possible security threats of information perception of IoT, but also realizes easily without changing any hardware conditions. In addition, our protocol can not only be applied to IoT authentication, but also be applied to any scene that needs to protect privacy data and sensitive data. In order to improve algorithm security, the future work may improve the algorithm by applying the lightweight encryption algorithm.

Acknowledgement: This work is supported by the National Science Foundation of China (Grant No. 61501132, Grant Nos. 61771154, 61301095, 61370084), the China Postdoctoral Science Foundation No. 2016M591515, the Heilongjiang Postdoctoral Sustentation Fund with No. LBH-Z14055, Harbin Application Technology Research and Development Project (Grant Nos. 2016RAQXJ063, 2016RAXXJ013).

References

Amin, R.; Biswas, G. P. (2015): A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Networks*, vol. 36, pp. 58-80.

Balakrishnan, A.; Rino, P. C. (2016): A novel anomaly detection algorithm for WSN. *Fifth International Conference on Advances in Computing and Communications*, pp. 118-121.

Chang, I.; Lee, T. F.; Lin, T. H. (2015): Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks. *Sensors*, vol. 15, no. 12, pp. 29841-29854.

Choi, Y.; Lee, D.; Kim, J. (2014): Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, vol. 14, no. 6, pp. 10081.

Das, A. K.; Sharma, P.; Chatterjee, S. (2012): A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Journal of Network & Computer Applications*, vol. 35, no. 5, pp. 1646-1656.

Dodis, Y.; Reyzin, L. (2004): Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 523-540.

Fan, R.; Ping, L. D.; Fu, J. Q. (2010): A secure and efficient user authentication protocol for two-tiered wireless sensor networks. *Circuits, Communications and System*, pp. 425-428.

He, D.; Gao, Y.; Chan, S. (2010): An enhanced two-factor user authentication scheme in wireless sensor networks. *Ad Hoc & Sensor Wireless Networks*, vol. 10, no. 4, pp. 361-371.

He, D.; Kumar, N.; Chilamkurti, N. (2014): A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *International Symposium on Wireless and Pervasive Computing*, pp. 263-277.

Jiang, Q.; Kumar, N.; Ma, J. (2016): A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks. *International Journal of Network Management*, vol. 27, no. 3, pp. 254-160.

Jiang, Q.; Ma, J.; Lu, X. (2015): An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1070-1081.

Khurram, K. M.; Khaled, A. (2010): Cryptanalysis and security improvements of 'two factor user authentication in wireless sensor networks'. *Sensors*, vol. 10, no. 3, pp. 2450.

Kim, J.; Lee, D.; Jeon, W. (2014): Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks. *Sensors*, vol. 14, no. 4, pp. 6443.

LEE, C. C.; Li, C. T.; Chen, S. D. (2011): Two attacks on a two-factor user authentication in wireless sensor networks. *Parallel Processing Letters*, vol. 21, no. 1, pp. 21-26.

Lin, Y.; Zhu, X.; Zheng, Z. (2017): The individual identification method of wireless device based on dimensionality reduction and machine learning. *Journal of Supercomputing*, no. 5, pp. 1-18.

Moreover; Section (2013): An efficient biometric authentication protocol for wireless sensor networks. *International Journal of Distributed Sensor Networks*, vol. 2013, no. 4, pp. 1614-1617.

Park, Y.; Park, Y. (2016): Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks: *Sensors*, vol. 16, no. 12, pp. 2123.

Qazi, F. A. (2004): A survey of biometric authentication systems. *International Conference on Security and Management*, pp. 61-67.

Ramanujam, R.; Sundararajan, V.; Suresh, S. P. (2014): *Extending Dolev-Yao with Assertions*. Springer International Publishing.

Sahingoz, O. K. (2013): Large scale wireless sensor networks with multi-level dynamic key management scheme. *Journal of Systems Architecture*, vol. 59, no. 9, pp. 801-807.

Sathishkumar, J.; Patel, D. R. (2014): A survey on internet of things: security and privacy issues. *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20-26.

Wu, D.; Yan, J.; Wang, H.; Wu, D.; Wang, R. (2017): Social attribute aware incentive mechanism for device-to-device video distribution. *IEEE Transactions on Multimedia*, vol. 19, no. 8, pp. 1908-1920.

Yoon, E. J.; Yoo, K. Y. (2014): A biometric-based authenticated key agreement scheme using ecc for wireless sensor networks. *ACM Symposium on Applied Computing*, pp. 699-705.