Intelligent Automation And Soft Computing, 2018

Vol.24,no 3, 519–529

A User Authentication Protocol Combined with the Trust Model, Biometrics and ECC for Wireless Sensor Networks

Tao Liu, Gan Huang*, Ping Zhang

School of Computer and Information, Anhui Polytechnic University, Wuhu, China

ABSTRACT

In this article, a new user authentication protocol using trust model, elliptic curve cryptography and biometrics for WSNs is submitted. The result of the trust model analysis indicates that the model can improve the model's ability of withstanding attacks from the malicious nodes. The results of safety analysis and performance analysis for our proposed user authentication protocol demonstrate that this protocol can be flexible to all sorts of common known attacks and performs similarly or better compared with some active user authentication protocols. It is suitable for WSNs which have a prominent request for the security and the performance.

KEY WORDS: U**ser authentication, Ant colony algorithm, Biometrics, Elliptic curves cryptography (ECC), Trust model, Wireless sensor networks (WSNs)**

1 INTRODUCTION

WIRELESS sensor networks, which consists of many sensor nodes, which are limited in computation, storage and energy, can inspect and gather data in the distributed area, then process and transport data to users ultimately. For the characteristics of powerful self-organization and flexible network topology structure of WSN, it has been widely applied in the fields of military affairs, industries, real-time traffic monitoring, measurement of seismic activity, wildlife monitoring and etc. (Chong & Kumar, 2003). The data may be sent to users through queries. Most of the queries are often issued at the points of base stations or gateway (GW) nodes in WSN applications. Nevertheless, there are great needs to access the real-time data from sensor nodes. Therefore, real-time data may no longer be accessed, only through base stations or GW nodes. The data can be accessed from sensor nodes by external users (Li, 2009).

Compared with traditional networks, for the characteristics of dynamic topology, opening channel and etc., the WSN is more vulnerable to be attacked, captured and destroyed. But for military or high-tech applications, the data collected is confidential or valuable. Authentication is the first line of defense for a security system. The characteristics of itself determine the traditional security authentication mechanism, and can't fit very well into their security needs. Therefore, it is necessary to find a suitable security and authentication scheme for sensor networks (Radi, Dezfouli, Bakar, 2012).

In 2002, Adrian Perrig et al. (Adrian, Robert, & Tygar, 2002) proposed a kind of security protocols for sensor network, one of secure network encryption protocol (SNEP) using symmetric cryptography to realize the communication of confidentiality, integrity and point-to-point authentication. Two keys used for encryption and authentication of a node to the base station are derived by the same algorithm as the main key shared with the base station. The shared secret key between nodes is temporarily allocated by the base station. WSN user entity authentication of public key system is proposed for the first time in (Watro, Kong, & Cuti, 2004), but the anti-capture property of this protocol is poor. Literature (Malan, Welsh, & Smith, 2004) based on the elliptic curve cryptosystem algorithm of the strong user authentication protocol for the document program has been improved. Wong et al. (Wong, Zheng, &Cao, 2006) put forward a

CONTACT Gan Huang ahczhg@skku.edu

dynamic user authentication protocol for WSNs by means of the hash function and exclusive-OR mathematical operation. This protocol saves computer loads and decreases the complexity of the computation. However, Das et al. (Das, 2009) stressed that Wong et al.'s protocol didn't keep a look out replaying attacks and impersonating attacks and an enhanced two-factor user authentication protocol for WSNs is proposed. It not only avoids the replay attacks and stolen-verifier attacks, but also defends against the code-guessing attacks and masquerade attacks. However, it doesn't defend the off-line code-guessing attacks and node compromising attacks, and it doesn't prevent the response information from the sense node to the user. In addition, it lacks mutual authentication.

In order to enhance the performance and the security of Das et al.'s protocols, A user authentication protocol for WSNs through employing elliptic curve cryptography is proposed by Yeh et al. (Yeh, Chen, & Liu, 2011) and Choi et al. (Choi, Lee, Kim, 2014). Compared with other cryptographies, it can reach the identical security with a key in a rather smaller size. Therefore, ECC is quite suitable for WSNs. Recently; Xue et al. (Xue, Ma, Hong, 2013) proposed a user authentication protocol for WSNs. In this protocol, a temporal credential produced by GW is distributed to the user and the sensor nodes. Through the method, the user, the sensor node and the gateway can achieve the mutual authentication between all of them. Besides, hash function and XOR operations are only used. But it is which only using simple passwords infeasible for WSNs to use the traditional authentication mechanisms, because of the differences lying among various networks. Our proposed user authentication protocol absorbs the merits of the above protocols and increases the trust model to enhance the performance of the above protocols and the accuracy of the authentication between entities.

2 REALTED WORK

2.1 Biometric Authentication

BIOMETRIC authentication technology as a means of identity authentication has become more widely used, such as the fingerprint attendance system, etc. Biometric identity authentication system is based on users' biological physiological structure features and behavior patterns for authentication. Because these biological characteristics are on the physiology and behavior associated with the user directly, biometric keys have some advantages, as follows: (YUAN, JIANG, JIANG, 2010).

(1) They are very difficult to copy with or share.

(2) They are not easy to drop out nor to forget.

(3) They are extremely hard to guess.

(4) They cannot be forged or distributed easily.

Therefore, compared with the traditional identity authentication system based on password, using the latest biometric identification technology of identity authentication system can provide better security (Long, 2015).

2.2 BAN-logic

Formal analysis for security protocols has widely gained attention in the field of security information. BAN logic is one of formal analysis methods for security protocols, which can be used to find protocol vulnerabilities based on formal analysis (QING, 2003).

Ban is a modal logic based on belief. In the process of BAN inference, participants' belief in a protocol would be changed along with the message exchanged. When BAN is applied, it should idealized the steps, which transform protocol messages to the formal Logic formula of BAN; next, they make rational assumptions according to the specific situation, and reasoning for the assumptions based on logic rules and Idealized protocols; in the end, it gets results whether the reasoning protocols meet with expected goals (HAN, & DING, 2011, Syverson & Oorschot, 1994).

BAN logic tries to answer the following questions:

(1) What the protocols can accomplish for goals?

(2) What is the assumption for the protocols?

(3) Whether there is redundant information for the protocols?

Whether to encrypt the message in the protocols can be passed using clear key without affecting the protocols' security?

BAN logic discusses abstractly the security for the certification agreement. Therefore, it cannot consider the security defects, which are induced by a specific implementation and the protocol defects, which are induced by the encryption system. On the whole, the BAN logic system makes the following assumptions:

(1) Blocks of cipher text cannot be tampered with, and several blocks of smaller cipher cannot compose a bigger block of cipher text.

(2) Two blocks of cipher text in a message are regarded as two arrive, respectively.

(3) Cipher Key Assumption, always assumes that the encryption system is perfect, that is to say, only the principal of the master key could understand the cipher text messages. A cipher key that does not have the right key cannot decode the cipher texts that are generated by the right cipher key. With the correct key to decrypt the cipher text is to definitely have a clearer meaning, and the wrong key decryption expressly does not make sense.

(4) The cipher text contains plenty of redundant information, which makes the whistleblower being judged whether he used the correct key.

(5) The message contains plenty of redundant information, which makes the principal being judged whether the message comes from itself.

(6) Principal Assumption, BAN logic assumes that the principal of the participation agreement is honest.

(7) Time Assumption, two times in protocol analysis are past-time and current-time. Current-time starts at the beginning of this agreement running stage, and before this is past-time. If a viewpoint is at the beginning of the agreement, so the current-time is established. However, the vice may not set up. Therefore, using time to distinguish can prevent message replay.

As a many-sorted modal logic, BAN logic mainly includes three process objects; principal, keys, and formula. The formula also can be named statement. BAN logic only contains proposition conjunction, which can be represented as a comma. The conjunction meets the exchange law and the combining law. According the rules of BAN logic, P, Q, and R represents the variable of principle; K represents the variable of keys and X, Y represents the variable of formula, respectively. A, B represents the normal principal, and S is the certificate server. $K_{ab}, K_{a;}, K_{b;}$ represents specific shared keys; K_a, K_b, K_c represents specific public keys; $K_a^{-1}, K_b^{-1}, K_c^{-1}$ represents specific private keys; N_a, N_b, N_c represents a temporary variable; h(X) represents the one-way hash function. We would introduce the inference of formal analysis of BAN logic as follows:

The goal of formal analysis tool based on the BAN logic system resolves the following questions:

(1) Whether the authentication protocol is correct;

(2) Whether the goal of the authentication protocol is attained;

(3) Whether the initial of the authentication protocols is appropriated;

(4) Whether the authentication protocol is redundant?

3 TRUST MODEL BASED ON OPTIMIZED ANT COLONY ALGORITHM

AT present, a series of studies were launched around the trust model of WSNs. However, the traditional trust model based on the biology algorithm for WSNs (BTRM-WSN) model has some demerits, such as high complexity and inaccurate trust calculation (Pan, Yu, &Yan, 2013, Mármol, & Pérez, 2011). In order to address these issues; a Trust Model Based on Optimized Ant Colony Algorithm [23] is proposed. This model is composed of the pheromone update, the path quality assessment, the trust evaluation and the punishment and reward mechanism. In addition, in order to enhance the accuracy of the global pheromone calculation, when the global pheromone is calculated, the optimal solution retention strategy is introduced into the trust model.

3.1 Principle of the Ant Colony Algorithm

In fact, the ant colony algorithm is a simulation of the real ant colony behavior of the simulated evolutionary algorithm (FENG & CHEN, 2014), and it is a randomized algorithm that is based on the natural world and the ant colony foraging behavior. When the ants are out in action, they release in its path through a special secretion called pheromones, and what`s more, ants can sense the substance to guide the direction of their movement. So the more the ants go through the certain path, the more pheromone is left on the path behind. Thus the probability of choosing the path is greater when other ants are out for food, then the later ants added the ant pheromone at the same path and this phenomenon forms a positive feedback mechanism, and finally the whole ant colony finds the optimal path.

3.2 Update of the Pheromone

The definition of the pheromone is as follows:

Define 1. The value of the pheromone means the trust between nodes, using $\tau_{ij}(t)$ in time t. Initially, m ants are put on n initiate nodes and the first element of the tabuk of every ant sets the original node. In the beginning, the pheromone of every track is equal, that is to say, $\tau_{ij}(0) = C$(C is a small constant).

Each ant based on pheromone value on the path determines the next node. The probability of ant k transferring from node i to node j is $p_{ij}^k(t)$ is as follows:

$$p_{ij}^k(t) = \begin{cases} \frac{\tau_{ij}(t)}{\sum_{r \in J_k(i)} \tau_{ir}(t)} & \text{when } j \in J_k(i) \\ 0 & \text{or not} \end{cases}, \quad (1)$$

$J_k(i)=\{1,2,\ldots n\}$- $tabu_k$ symbolizes the set of next nodes ant k can choose. When ant k passes a node, it puts this node into $tabu_k$.

The update of the pheromone consists of the local pheromone update and global pheromone update. Each ant passing one node every time will carry out a local pheromone update. When an ant transfers from a node i to a node j, the side ij will update the value of the pheromone as follows:

$$\tau_{ij}(t+1) = (1-\rho)\tau_{ij}(t) + \rho\tau_0 \quad , \quad (2)$$

ρ is an evaporation factor of the pheromone on the path, enabling the path to forget a bad situation in order to avoid the path into a sub-optimal situation. τ_0 is an initiate value of the pheromone on the path? The role of the local pheromone update is that when the ants have found the pheromone of the selected side reduces, it will turn to choose sides, which are not chosen.

After each iteration the global pheromone of the optimum path all the ants have found will be updated. The global pheromone of the optimal path ij is updated as follows:

$$\tau_{ij}(t+1) = (1-\rho)\tau_{ij}(t) + \rho\Delta\tau_{ij} + \Delta\tau_{ij}^{*} \quad , \quad (3)$$

$$\Delta\tau_{ij} = \sum_{k=1}^{m} \Delta\tau_{ij}^{k} \quad , \quad (4)$$

$$\Delta\tau_{ij}^{k} = \begin{cases} \frac{Q}{L_k} & \text{when ant k pass the side ij} \\ 0 & \text{or not} \end{cases} \quad , \quad (5)$$

$$\Delta\tau_{ij}^{*} = \begin{cases} \sigma * \frac{Q}{L_{g_b}} & \text{if side ij is a part of the optimal way} \\ 0 & \text{or not} \end{cases}, \quad (6)$$

L_k is the length of the path ant k travels in this iteration, $\Delta\tau_{ij}^{*}$ is the increasing pheromone of the path ij the optimal ant passes, σ is the number of the optimal ants, L_{g_b} is global optimal solution.

3.3 Path Quality Assessment

Each time the ants return the source node after one iteration they will remember the path they traversed. After that, the source node will evaluate the quality of the path this ant passed. Especially ants hold node lists and pheromone on the path. The calculation of the path quality assessment is as follows:

$$Q(S_k) = \frac{\overline{\tau_k}}{\text{Length}(S_k)^{PLF}} * A_k \quad , \quad (7)$$

$\overline{\tau_k}$ is the average pheromone of the path the ant k found, PLF ∈ [0,1], A_k is the radio of the number of ants selecting the same path with the ant k. By the above method, ants in the trust model will choose the shorter path as much as possible, and will choose this path many times.

3.4 Trust Evaluation

In the networks, every node maintains a set of pheromones, determining which path ants will choose. Nevertheless, pheromone values are often confused with trust values. In order to differentiate the two concepts, T_i is used to signify the trust of node i. The calculation process is as follows:

$$T_i = \sum_{j=1}^{j\in I(i)} \frac{\sin(\tau_{ij})}{|I(i)|} \quad , \quad (8)$$

I(i) means the nodes having a way to the node i. Each node will maintain a trust list on the neighbor nodes.

3.5 NPunishment and Reward Mechanism

For the sake of enhancing the accuracy of the trust model and preventing the attack of the malicious node, "addition increase, multiplication decrease" is carried out after the trust evaluation is finished. The process is as follows:

$$T_i = \begin{cases} T_{max} & \text{uppper limit} \\ T_i + \text{step} & \text{When the communication is good,} \\ \tau * T_i & \text{When the communication is not good} \end{cases} \quad (9)$$

T_w is a trust threshold. If $T_i > T_W$, the communication is good. Otherwise, the communication is not good.

4 THE PROPOSED PROTOCOL

BASED on the descriptions and explanations on the above protocol, a new enhanced user authentication protocol integrated with biometrics is proposed in an effort to solve the weaknesses. Before analysis, the notations with their corresponding meanings are summarized in Table 1 first.

Our proposed protocol can be illustrated step by step.

4.1 Registration Phase

In this phase, the user U submits an identity ID_U, and a hash password $\overline{PW_U}$ to the GW node in a secure way. Then, the GW node issues a smart card to U. Its description is as follows:

1. The user U selects his/her identity ID_U and password PW_U freely, inputs his/her personal biometrics B_U (fingerprint, etc.) and computes $f_U = h(B_U), \overline{PW_U} = h(PW_U \oplus f_U)$.U sends ID_U and $\overline{PW_U}$ to GW via a secure channel.

2. Once received, GW computes $K_U = h(x||y||ID_U) \times P$ and $W_U = h(ID_U||\overline{PW_U}||f_U) \oplus K_U$.Then GW saves $\{W_U, \overline{PW_U}, h(\cdot)\}$ into a smart card and transmits it to the user U via a secure channel.

4.2 Login Phase

In order to access data from WSNs, U should provide his/her B_U', ID_U' and PW_U'. The smart card goes through the subsequent steps to confirm the justifiability of U.

(1) U inserts his/her smart card into the terminal and inputs personal biometrics B_U', identity ID_U' and password PW_U'.

(2) The smart card computes

$f_U' = h(B_U')$ and $\overline{PW_U}' = h(PW_U' \oplus f_U')$, and checks whether

$$\overline{PW_U}' = \overline{PW_U}$$

If the equation is incorrect, the smart card refuses the demand. Or else, the smart card chooses randomly a number $\gamma_U \in Z_q^{*}$ and calculates

$$\begin{aligned} K_U &= W_U \oplus h(ID_U \oplus \overline{PW_U}||f_U), X \\ &= \gamma_U \times P, X' \\ &= \gamma_U \times K_U, \omega \\ &= h\left(ID_U \left|\left|ID_{S_n}\right|\right| x||y||T_U\right), \\ \alpha &= h(ID_U||ID_{S_n}||X||X'||T_U||\omega), \end{aligned}$$

where T_U is the current timestamp of the user U. Finally, U sends $M_1 = \{ID_U, ID_{S_n}, X, T_U, \alpha, \omega\}$ to the gateway GW.

(1) S_n first verifies if $T'' - T_U \le \Delta T$ and $T'' - T_G \le \Delta T$. If the requirement is reached, the validity of ΔT and T_G can be guaranteed. Then S_n can pursue the next step. Otherwise, S_n refuses to carry on.

Table 1. Notations.

Symbol	Mean
p, q	Two large prime numbers
U	A user
ID_U	A user's identity
ID_{S_n}	The identity of sensor node S_n
PW_U	The password of user U
B_U	Biometric template of user U
x, y	The master keys of GW node
$h(\cdot)$	An anti-collision one-way hash function
$\|\|$	A string connector
$\oplus$	A string XOR operation
F_p	A finite field
P	A point on elliptic curve E with an order n

(2) Then S_n tests whether $\beta = h(ID_U||X||T_U||\alpha||\omega||ID_{S_n})$. If the equation doesn't correspond, S_n terminates the authentication. Or else, S_n calculates $X' = h(ID_U||x||y) \times X$ Then S_n checks if $\alpha = h(ID_U||X||T_U||X'||\omega||ID_{S_n})$. If the check fails, the authentication ends. Otherwise, it produces a random number $\gamma_a \in Z_q^*$, computes $Y = \gamma_a \times P$ and gets the current timestamp T_{S_n} and computes $\gamma = h(ID_U||X||\alpha||ID_{S_n}||Y||T_{S_n})$.

In the end, S_n node sends $M_3 = \{T_{S_n}, \gamma, \delta\}$. Once receiving M_3 at T''', GW performs to authenticate sensor S_n as follows:

(1) GW tests whether $T''' - T_{S_n} \leq \Delta T$. If the condition is reached, the validity of T_{S_n} can be committed and S_n can proceed. If not, S_n refuses the request.

(2) GW checks whether $\gamma = h(ID_U||X||\alpha||ID_{S_n}||Y||T_G)$. If the answer is no, the authentication ends. Otherwise, GW gets the current timestamp T_G' and transfer M4=$\{T_G'\}$ to Sn.

When getting M4 at T'''' ,S_n proceeds as follows:

(1) S_n checks whether $T'''' - T_G' \leq \Delta T$. If not, Sn terminates the following process. Otherwise, S_n computes $K_{SU} = \gamma_a \times X$ and the session key SK=$h(X||Y||K_{SU})$.

(2) S_n gets the current timestamp T_{S_n}'.Then S_n sends $M_5 = \{Y, T_{S_n}'\}$ to U.

Upon receiving M_5, U operates the below process.

U checks if $T'''' - T_{S_n}' \leq \Delta T$. If M_5 is not fresh, U stops the session; otherwise, U inquires the trust of sensor S_n and checks if $T_i(S_n) > T_W$. If not, U stops the session; otherwise, U computes $K_{US} = \gamma_U \times Y$ and gets session key SK= $h(X||Y||K_{US})$. U and S_n can make sessions.

4.3 Password Update Phase

When the user wants to reset his password, the password update phase happens. The password update phase is explained below.

(1) The user inserts his/her smart card into the terminal and enters the biometric templates B_U, the identity ID_U, the old password PW_U and a new one PW_U'.

(2) The smart card checks if $f_U = h(B_U)$. If the answer is no, U rejects the demand. Otherwise, the smart card computes $\overline{PW_U}' = h(PW_U \oplus f_U)$. The smart card checks if $\overline{PW_U}' = \overline{PW_U}$. If the equation doesn't hold, the password update phase is over. Otherwise, the smart card calculates $K_U = W_U \oplus h(ID_U||\overline{PW_U}||f_U), \overline{PW_U}' = h(PW_U' \oplus f_U)$ and $W_U' = h(ID_U||\overline{PW_U}'||f_U) \oplus K_U$ and replaces $W_U, \overline{PW_U}$ with W_U', $\overline{PW_U}'$, correspondingly.

5 TRUST MODEL ANALYSIS

WITH the aim of assessing the performance and reliability of the proposed trust model, this paper is compared with BTRM-WSN models throughout three simulations using TRMSim-WSN (Mármol, Pérez,2009). The first set of experiments compares the two models in the

accuracy of the search trusted node. The second set of experiments compares the two models for the average path length for finding the required trusted node. The third set of experiments compares the total energy the two models consume.

5.1 TRMSim-WSN

TRMSim-WSN is a Java-based wireless sensor network trust model simulation, which provides a very convenient way to test the trust model. In order to simulate two trust models, some parameters need setting as; Client: 15%, Relay Server: 6%, Radio Range: 10, Min Num Sensors and Max Num Sensors: 100, Num networks: 400, Number executions: 100. Then, the simulator will randomly generate a wireless sensor network based on these parameters. Note that 85% of the nodes are server nodes to provide the service.

5.2 Accuracy

THE exact rate of the trust model was used to estimate the reliability and safety of the trust model, which uses the ratio of the number of credible sensor nodes the trust model chooses successfully to the total number of treatments. A good trust model is able to have good control over the malicious node attacks. The accuracy of the trust model and the accuracy of the BTRM-WSN were compared in Figure 1. It can be seen over the figure that when the ratio is less than 50 percent of malicious nodes, the two trust models on the accuracy of finding the credible nodes is similar. However, when the ratio of malicious nodes is higher than 50 percent, the proposed model can provide higher accuracy and security than the BTRM-WSN.

5.3 Energy Consumption

The wireless sensor network is an energy-limited network, so a designed trust model for the wireless sensor network is required to reduce energy consumption to ensure network security and enlarge the life cycle of the networks. Energy expenditure in the wireless sensor network includes the energy source nodes that are consumed in sending information and the energy consumed by malicious nodes providing malicious service and the energy consumed in order to search trusted nodes in the networks. Figure 2 is a comparison of two trust models in energy consumption. As shown, the energy consumption of the trust model proposed is less than the BTRM-WSN, so the proposed trust model is more suitable for the wireless sensor network.

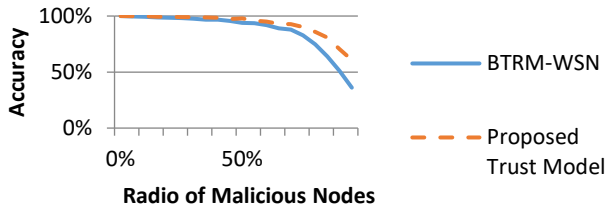

Figure 1. Comparison of Accuracy.

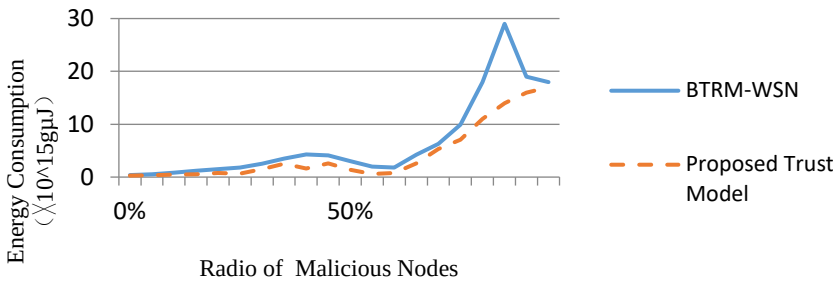

Figure 2. Comparison of Energy Consumption.

6 SECURITY ANALYSIS

IN this section, the security of our proposed protocol for WSNs will be analyzed using BAN-logic.

6.1 Analysis of the Proposed Protocol Using BAN-logic

In this subsection, BAN-logic (Burrows, Abadi, Needham, 1989) is used to analyze the proposed protocol. First of all, some notations and statements are shown as follows: Where X, Y and K symbolize statements and P signifies a principal.

- (X, Y): conjunction of two statements X and Y.
- $\{X\}_{+K}$: X is encrypted with the key K.
- $\{X\}_{-K}$: X is decrypted with the key K.
- $(X)_K$: X is hashed throughout the key K.
- $<X>_Y$: X combined with Y.
- #(X): X is fresh.
- $P| \equiv X$: P believes X and will continue to do something for the rest of the protocol.
- P =>X: P has jurisdiction over X and should be trusted as to X.
- P|~X: P once conveyed X. SK:The session key shared between U and S_n
- In addition, some main logic postulates of the BAN-logic are described as follows, which will be used in our analysis.
- The message-meaning rule: $\frac{P| \equiv P \overset{K}{\leftrightarrow} Q, P \nabla \{X\}_k}{P| \equiv Q| \sim X}$.
- The freshness-conjunction rule: $\frac{P| \equiv \#(X)}{P| \equiv \#(X,Y)}$.
- The nonce-verification rule: $\frac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$.
- The jurisdiction rule: $\frac{P| \equiv Q => X, P| \equiv Q| \equiv X}{P| \equiv X}$.

Our proposed user authentication protocol needs to meet the following goals.

Goal 1. $U| \equiv (U \overset{SK}{\leftrightarrow} S_n)$

Goal 2. $U| \equiv S_n| \equiv (U \overset{SK}{\leftrightarrow} S_n)$

Goal 3. $S_n| \equiv (U \overset{SK}{\leftrightarrow} S_n)$

Goal 4. $S_n| \equiv U| \equiv (U \overset{SK}{\leftrightarrow} S_n)$

Goal 5. $U| \equiv \left(U \overset{ID_U}{\longleftrightarrow} S_n\right)$

Goal 6. $U| \equiv S_n| \equiv (U \overset{ID_U}{\longleftrightarrow} S_n)$

Goal 7. $S_n| \equiv (U \overset{ID_U}{\longleftrightarrow} S_n)$

Goal 8. $S_n| \equiv U| \equiv (U \overset{ID_U}{\longleftrightarrow} S_n)$

First of all, it's necessary to make some assumptions in order to derive our goals.

A1: $U| \equiv \#(T_U)$

A2: $U| \equiv \#(\gamma_U)$

A3: $U| \equiv \#(T'_{S_n})$

A4: $U| \equiv U \overset{\omega=h(ID_U||ID_{S_n}||x||y||T_U)}{\longleftrightarrow} GW$

A5: $U| \equiv S_n => U \overset{SK}{\leftrightarrow} S_n$

A6: $U| \equiv S_n => U \overset{ID_U}{\longleftrightarrow} S_n$

A7: $GW| \equiv \#(T_U)$

A8: $GW| \equiv U \overset{\omega}{\leftrightarrow} GW$

A9: $GW| \equiv S_n \overset{\beta=h(ID_U||X||T_U||\alpha||\omega||ID_{S_n})}{\longleftrightarrow} GW$

A10: $S_n| \equiv \#(T_U)$

A11: $S_n| \equiv \#(T_G)$

A12: $S_n| \equiv \#(T'_G)$

A13: $S_n| \equiv GW => U \overset{SK}{\leftrightarrow} S_n$

A14: $S_n| \equiv GW => U \overset{ID_U}{\longleftrightarrow} S_n$

A15: $S_n| \equiv U => U \overset{SK}{\leftrightarrow} S_n$

A16: $S_n| \equiv U => U \overset{ID_U}{\longleftrightarrow} S_n$

Second, the proposed protocol needs to be transformed into the idealized form.

Msg1. $U \rightarrow GW: (T_U, U \overset{ID_U}{\leftrightarrow} S_n, U \overset{\gamma_U}{\leftrightarrow} S_n)_{h(ID_U||\overline{PW_U}||f_U)}$

Msg2. $GW \rightarrow S_n: T_G, U| \equiv U \overset{ID_U}{\longleftrightarrow} S_n, U| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n$

Msg 3. $S_n \rightarrow GW: T_{S_n}, U| \equiv U \overset{ID_U}{\longleftrightarrow} S_n, U| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n$

Msg 4. $GW \rightarrow S_n: T'_G, U| \equiv U \overset{ID_U}{\longleftrightarrow} S_n, U| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n$

Msg 5. $S_n \rightarrow U: T'_{S_n}, U \overset{ID_U}{\longleftrightarrow} S_n, U \overset{\gamma_U}{\leftrightarrow} S_n$

Third, the idealized outline of the proposed protocol is analyzed using the BAN logic. The chief steps are depicted as follows:

By Msg 1, it is easy to reach the statement as follows:

S_1: $GW \triangleleft (T_U, U \overset{ID_U}{\longleftrightarrow} S_n, U \overset{\gamma_U}{\leftrightarrow} S_n)_{h(ID_U||\overline{PW_U}||f_U)}$.

By A9, S_1 and the message-meaning rule it is easy to achieve

S_2: $GW| \equiv U|\sim(T_U, U \overset{ID_U}{\longleftrightarrow} S_n, U \overset{\gamma_U}{\leftrightarrow} S_n)$.

By A7, S_2 and the freshness-conjunction rule, it is easy to achieve

S_3: $GW| \equiv U| \equiv(U \overset{ID_U}{\longleftrightarrow} S_n, U \overset{\gamma_U}{\leftrightarrow} S_n)$.

By S_3 and the belief rule, it is easy to get

S4: $GW| \equiv U| \equiv(U \overset{ID_U}{\longleftrightarrow} S_n)$

S5: $GW| \equiv U| \equiv(U \overset{\gamma_U}{\leftrightarrow} S_n)$

By Ms 2, 3, 4, it is easy to achieve

S6: $S_n \triangleleft(T_G, T_G', U| \equiv U \overset{ID_U}{\longleftrightarrow} S_n, U| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n)$

S7:$G2\triangleleft(T_{S_n}, U| \equiv U \overset{ID_U}{\longleftrightarrow} S_n, U| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n)$

By A13, A14, S6 and message-meaning rule, it is easy to achieve

S8: $S_n|\equiv GW|\sim(T_G, T_G', U| \equiv U \overset{ID_U}{\longleftrightarrow} S_n, U| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n)$

By A10,A11, A12, S6 and the freshness-conjunction rule, it is easy to achieve

S9: $S_n|\equiv GW| \equiv (U| \equiv U \overset{ID_U}{\longleftrightarrow} S_n, U| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n)$

By S9 and the belief rule, it is easy to achieve

S10: $S_n|\equiv GW| \equiv (U| \equiv U \overset{ID_U}{\longleftrightarrow} S_n)$

S11: $S_n|\equiv GW| \equiv (U| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n)$

By A14, S10 and the jurisdiction rule, it is easy to attain

S12: $S_n|\equiv U| \equiv (U \overset{ID_U}{\longleftrightarrow} S_n)$(*Goal 8*)

By A16, S11 and the jurisdiction rule, it is easy to attain

S13: $S_n| \equiv (U \overset{ID_U}{\longleftrightarrow} S_n)$(*Goal 7*)

By A13, S10 and the jurisdiction rule, it is easy to attain

S14: $S_n| \equiv U| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n$

Since $SK= h(X||Y||K_{US})$,it is easy to attain

S15: $S_n|\equiv U| \equiv (U \overset{SK}{\leftrightarrow} S_n)$(*Goal 4*)

By A15, S15 and the jurisdiction rule, it is easy to attain

S16: $S_n| \equiv (U \overset{SK}{\leftrightarrow} S_n)$(*Goal 3*)

By Msg 5, it is easy to achieve

S17: $U\triangleleft(T_{S_n}', U \overset{ID_U}{\longleftrightarrow} S_n, U \overset{\gamma_U}{\leftrightarrow} S_n)$

By A8, S17 and the message-meaning rule, it is easy to say attain

S18: $U| \equiv S_n|\sim(T_{S_n}', U \overset{ID_U}{\longleftrightarrow} S_n, U \overset{\gamma_U}{\leftrightarrow} S_n)$

By A3, S18 and the freshness-conjunction rule, it is easy to attain

S19: $U|\equiv S_n| \equiv (U \overset{ID_U}{\longleftrightarrow} S_n)$(*Goal 6*)

By A6, S19 and the jurisdiction rule, it is easy to achieve

S20: $U| \equiv (U \overset{ID_U}{\longleftrightarrow} S_n)$(*Goal 5*)

By A3, S18 and the freshness-conjunction rule, it is easy to attain

S21: $U| \equiv S_n| \equiv U \overset{\gamma_U}{\leftrightarrow} S_n$

Since $SK= h(X||Y||K_{US})$, it is easy to attain

S22: $U|\equiv S_n| \equiv (U \overset{SK}{\leftrightarrow} S_n)$(Goal *2*)

By A5, S22 and the jurisdiction rule, it is easy to say

S23: $U| \equiv (U \overset{SK}{\leftrightarrow} S_n)$(*Goal 1*)

Throughout (Goal 1), (Goal 2), (Goal 3), (Goal 4), (Goal 5), (Goal 6), (Goal 7), (Goal 8), it is indicated that both U and S_n believe that a session key SK and an identity ID_U are shared between them.

6.2 Other Discussion

THE OREML. The proposed user authentication protocol can assist a stolen-verifier attack and many users who suffer from the same login-id attack, man-in-the-middle attack, the session key attack, the stolen smart card attack and the sensor energy exhausting attack.

1. Stolen-verifier Attack: An attacker can do the stolen-verifier attack if the GW nodes stores verifier tables for authentication. However, our proposed protocol doesn't need any verifier tables. Therefore, it's impossible that the stolen-verifier attack happens.

2. Many Users who suffer from the Same Login-id Attack is when the user wants to go through the login process to WSNs. Our proposed protocol requires the user to provide his/her identity ID_U, the password PW_U, and his/her personal biometrics B_U. It is noted that $\overline{PW_U}$ is in alliance with $f_U = h(B_U)$. Though two attackers may have the same identity ID_U and the same password PW_U, their biometrics B_U and $\overline{PW_U} = h(PW_U \oplus f_U)$ are distinct. Therefore, our proposed protocol can defend this attack.

3. Session Key Attack: In a session key attack, an attack intercepts the user's sending

authentication message and constructs a session key with the user. In our proposed protocol, $\alpha = h(ID_U||ID_{S_n}||X||X'||T_U||\omega)$ consists of ID_U and ID_{S_n} denoting the user wanting to communicate with the sensor node S_n. GW node uses $\delta = h(ID_U||X||X'||T_U||Y||T_{S_n})$ denoting GW node has authenticated the status of the user U and the sensor node S_n. The session key attack can be avoided by using a and δ.

7 PERFORMANCE ANALYSIS

TABLE 2 will contrast our proposed protocol with Yeh et al.'s protocol and Xue et al.'s protocol towards the computation cost. First, notations need to be illustrated as follows:

H: The time for calculating the hash function; X: The time for calculating the bit XOR; E: The time for calculating the bit ECC encryption/decryption. Table 2 of computer cost comparison is as follows:

As shown in Table 2, the total computational cost of three protocols is 8H+8E, 24H+13X and 14H+2X+6E respectively. Our protocol and Yeh et al.'s protocol have better capability than Xue et al.'s protocol in the S_n and the GW. In WSNs, our proposed protocol and Yeh et al.'s protocol can save energy consumption better and be more effective for the WSNs than Xue et al.'s protocol. The property of our protocol is analogous to that of Yeh et al.'s protocol. However, Yeh et al.'s protocol is flimsy to some common attacks. The proposed protocol in the article can contribute to the safety of the user authentication protocol. Therefore, the proposed protocol has better performance than other protocols.

Table 2. Computation Cost.

Protocol	Computation Cost		
	User	Sensor	Gateway
Yeh *et al.*'s protocol	H+2E	3H+2E	4H+4E
Xue *et al.*'s protocol	7H+5E	7H+5X	10H+3X
Our proposed protocol	6H+2X+3E	5H+3E	3H

8 CONCLUSION

IN this paper, a novel user authentication based on a trust model, biometrics and ECC is proposed in the WSN. Throughout the trust model analysis, the model shows higher accuracy and less energy consumption. Analysis throughout the BAN logic indicates the proposed user authentication protocol can attain higher security requirements as to user authentication in WSNs. Moreover, it can resist a variety of attacks. Performance evaluation indicates that the proposed protocol has better performance than Xue et al.'s protocol and Yeh et al.'s protocol. In the future, the current work towards the WSNs will be hereby extended.

9 ACKNOWLEDGMENT

THIS work was supported by the National Natural Science Foundation of China (No. 61300170, No. 61501005), the University Provincial Natural Science Foundation of Anhui Province (No.KJ2016A057), the Natural Science Foundation of Anhui Province under Grant (No. 1608085MF147).

10 REFERENCES

M. Burrows, Abadi M, and Needham R M., (1989). *A logic of authentication, Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences. The Royal Society*, 426(1871): 233-271

Y. Choi, Lee D, Kim J, et al., (2014). *Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography*, *Sensors*, 14(6): 10081-10106.

C. Y. Chong & Kumar S. (2003). *Sensor networks: Evolution, opportunities and challenges, Proceedings of IEEE*. 91(8), 1247-1256.

M. L. Das, (2009). *Two-factor user authentication in wireless sensor networks[J]. Wireless Communications, IEEE Transactions on*, 8(3): 1086-1090.

M. Dorigo & Blum C., (2005). *Ant colony optimization theory: A survey[J]. Theoretical computer science*, 344(2): 243-278.

Y-H. Feng & Chen Zhou-Ji, (2014). *The Principle and Application Research on Ant Colony Algorithm Based on Swarm Intelligence[J].Journal of Lanzhou University of Arts and Science(Natural Sciences)*.28(02):58-62.

H. Qiu-jun & Ding Yue-Wei, (2011). *Design and Analysis of New Authorization Schemein SaaSMode, Computer Engineering* 37(7):133-135

C. T. Li. (2009). *An enhanced remote user authentication scheme providing mutual authentication and key agreement with Smart Cards, The 5th International Conference on Information Assurance and Security, Xi'an: IEEE Computer Society*, 2009: 517-520.

DJ Malan, Welsh M, and *Smith MD*, et al., (2004). *A Public-key Infrastructure for Key Distribution in TinyOS based on Elliptic Curve Cryptography,Proceedings of the 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks, USA :IEEE Pres*s, 2004:71-80.

F. G. Mármol & Pérez G M., (2011). *Providing trust in wireless sensor networks using a bio-inspired technique[J]. Telecommunication systems*, 46(2): 163-180.

F. G. Mármol & Pérez G M., (2009). *TRMSim-WSN, trust and reputation models simulator for wireless sensor network, Communications, 2009. ICC'09. IEEE International Conference on. IEEE*, 2009: 1-5.

Y. Pan, Yu Y, and Yan L., (2013). *An improved trust model based on interactive ant algorithms and its applications in wireless sensor networks[J]. International Journal of Distributed Sensor Networks*, 2013(7):385-388.

A. Perrig, Robert Szewczyk, J. D. Tygar, et al.., (2002). *SPINS: security protocols for sensor networks, Journal Wireless Networks*, 8(5):521–534.

S-H. Qing. (2003). *Design and Logical Analysis of Security Protocols, Journal of Software*, 14(7):1300-1309

M. Radi, Dezfouli B, Bakar K A, et al., (2012). *Multipath routing in wireless sensor networks: survey and research challenges, Sensors, 2*012, 12(1): 650-685.

P. F. Syverson & *Oorschot* Paul C. van, (1994). *On Unifying Some Cryptographic Protocol Logics[C].Proceedings of the 1994 IEEE Computer Society Symposium on Security and Privacy. Oakland, USA: IEEE Computer Society Press*, 1994. pp:14-28

R. Watro, Kong D, Cuti S, et al., (2004). *Tiny PK: securing sensor networks with public key technology, Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM*, 2004: 59-64.

L. Wei, (2015). *Research on Anonymous Identity Authentication Based on Biometrics[D], BEIJING JIAOTONG UNIVERSITY*, 2015(4):2-13

K H M Wong, Zheng Y, Cao J, et al., (2006). *A dynamic user authentication scheme for wireless sensor networks, Sensor Networks, Ubiquitous, and Trustworthy Computing, IEEE International Conference on*. 2006: 1-8.

K. Xue, Ma C, Hong P, et al., (2013). *A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, Journal of Network & Computer Applications*, 36(1):316-323.

H. L. Yeh, Chen T H, Liu P C, et al., (2011). *A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors*, 11(5): 4767-4779.

J. Yuan, Jiang Changjun, Jiang Zuowen, et al., (2010). *A Biometric-Based User Authentication for Wireless Sensor Networks, WuHan University Journal of Natural Sciences*, 15 (3): 272-276

11 NOTES ON CONTRIBUTORS

Tao Liu is a professor. She received B.S. degree in Computer Application Technology from HeFei University of Technology, China in 2004. She was a visiting scholar at the University of Science and Technology of China in 2012. Her main

research interests include machine learning, computer network and Information security. Email:liutao@ahpu.edu.cn

Gan Huang received M.S. degree from the School of Computer and Information at Anhui Polytechnic University, China, in 2016. He is now studying at the Department of Electrical and Computer Engineering, Sungkyunkwan University for a Ph.D. degree. In his master's study, he worked on wireless sensor networks. His current research interests are in edge computing and software-defined networking. In this paper, he is corresponding author. Email:ahczhg@skku.edu

Ping Zhang received the B.S. degree in mathematics from Anhui Normal University, China, in 2004, the M.S. degree in statistics from Southeast University, China, in 2007, and the Ph.D. degree in the School of Information Science and Engineering from Southeast University, China, in 2015. His research interests include sensor network localization, network data mining, and statistical signal processing.