Journal of Software Engineering

ISSN 1819-4311

Academic Journals Inc.

www.academicjournals.com

Journal of Software Engineering 8 (3): 184-193, 2014
ISSN 1819-4311 / DOI: 10.3923/jse.2014.184.193

Secure and Efficient Mutual User Authentication Protocol for Wireless Sensor Networks

Qinghua Yang, Liejun Wang, Qi Liu and Mingwei Wang
Information Science and Engineering, Xinjiang University, Urumqi, China

Corresponding Author: Liejun Wang, Information Science and Engineering, Xinjiang University, Urumqi, China

ABSTRACT

Authentication is a very significant demand in wireless sensor networks, especially in some critical applications. However, most previous user authentication schemes are always vulnerable and high-power consumption for the resource-constrained WSNs nodes. This study will focus on user authentication by investigating the Park and others' schemes to identify their demerits. After that, a novel and lightweight mutual user authentication protocol named MUAP is proposed. The analysis and results show that the proposed scheme not only can resist the specific attacks likes Man-In-The-Middle Attack, Impersonation Attack and Message-Alteration Attack but also is better than Kumar and others' protocols in terms of devices' computation overhead and communication consumption.

Key words: Wireless sensor networks, mutual user authentication, session key, confidentiality

INTRODUCTION

Recent years, Wireless Sensor Network (WSN) grows rapidly in accommodating plenty of application areas. The applications include military, national security, environmental monitoring, traffic management, health care, manufacturing and so on (Kumar *et al*., 2013). The WSN consists of resource-constrained sensors Crossbow Technology (2012) and Moteiv Corporation (2012) that have low computational ability, low power, low bandwidth and a small amount of memory. The broadcast nature of the sensor node makes it possible for a user to access sensor data within the networks, that is, on demand users may misuse the sensitive data for personal reasons (Das, 2009, 2011; Sun *et al*., 2013). Since, the sensor data are private for users within the WSN, it is mandatory to authenticate the users before permitting access to the sensitive data. Therefore, user authentication is a primary concern in application areas of WSNs.

At present, some mutual user authentication protocols have been proposed for resource-constraint WSNs (Ko, 2008; Lee, 2008; Chen and Shih, 2010; He *et al*., 2010; Khan and Alghathbar, 2010; Yoo *et al*., 2012) and each of these protocols has its advantages and disadvantages. Gao proposed a two-factor user authentication protocol which is based on a smartcard and password in 2010 (He *et al*., 2010). However, Chen showed that Gao's protocol fails in mutual authentication and is vulnerable to parallel-session attacks. After that, they proposed a robust mutual authentication protocol for WSNs in (Chen and Shih, 2010). Khan proposed an improvement advice to Gao's scheme to resist these attacks.

In 2012, Park claimed that the protocols which are proposed in (Chen and Shih, 2010; He *et al*., 2010; Khan and Alghathbar, 2010) are sensitive to parallel-session attacks and

gateway-bypass attacks and are none of mutual authentication schemes. Therefore, they proposed a scheme (Yoo *et al*., 2012) to overcome the problem that presented in (Chen and Shih, 2010; He *et al*., 2010; Khan and Alghathbar, 2010).

Nevertheless, according to our study, Park and others' protocols are not only sensitive to impersonation attacks, message-alteration attacks and man-in-the-middle attacks but they are not efficient (in terms of communication and computation cost) for real-time WSNs. Therefore, we propose a strong and lightweight user authentication protocol that protects the privacy of the user, wherein each user has to demonstrate his legitimacy by show his secret information. The proposed scheme has many merits, including mutual authentication for entities (that is, sensor, gateway and user), protecting user's privacy and maintaining confidential wireless messages. Further, we show that the protocol we proposed is strong against popular attacks, in contrast to those in (Chen and Shih, 2010; He *et al*., 2010; Khan and Alghathbar, 2010) and obtains high efficiency at computation overhead and communication consumption.

ANALYSIS OF PARK AND OTHERS' SCHEME

Review of Park and others' protocol: The schemes of Park and other's are consist of three parts: Registration, authentication and password-change. The details of this protocol are shown in Fig. 1.

Registration part: To access the sensor data, each user has to register himself by passing his ID_U and $PPW_u = h(PW_u) \oplus b$ to Gateway nodes in a secure channel, where, b is a secret number generated by user. After that, the Gateway node uses the receiving data ID_u and PPW_u to calculate the following equations $M_u = h(ID_u \| PPW_u)$, $N_u = h(ID_u \| PPW_u) \oplus h(K \| J)$, $L_u = h \| (J_u \| ID_u)$, where, J is a random number generated by the Gateway node and K is a key generated by the Gateway node. Finally, the parameters $\{M_u, N_u, L_u, h(.)\}$ are passed to the user. The user adds b to the smartcard as his secret.

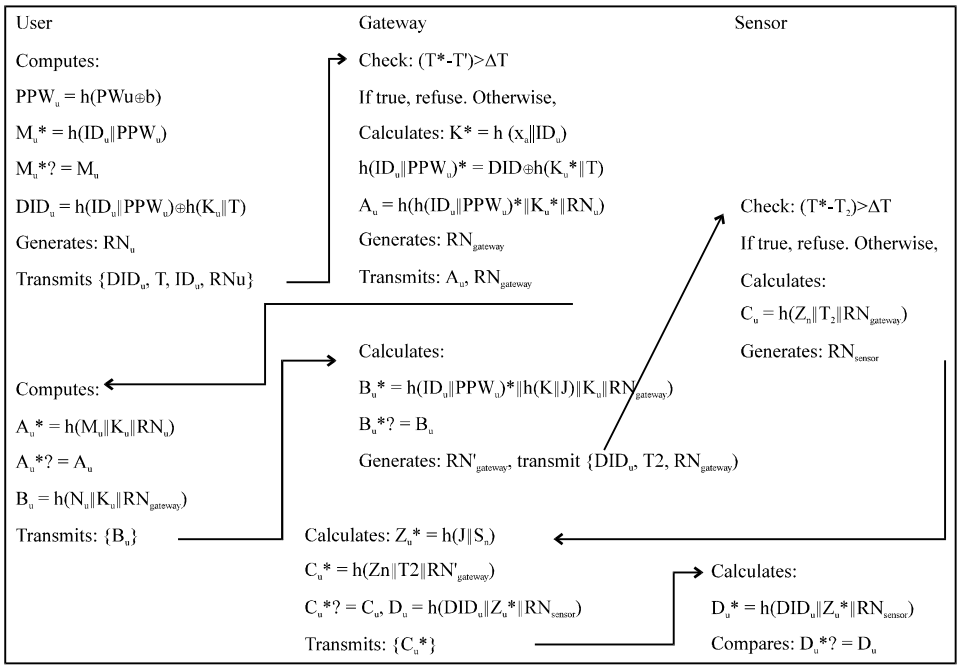

Fig. 1: Park and others' authentication part

Authentication part: This authentication part can be divided into three parts: Login part, verification part and session key establishment.

Login part: The user tries to access the sensor data on demand. The user has to use his smartcard and input his ID_u and PW_u. The smartcard performs series of computations after getting the request from user as the Fig. 1 shown.

Verification part: In this part, user and Gateway verified for each other by transmitting the data $\{A_u, RN_{gateway}\}$, $\{B_u\}$, $\{DID_u, T_2, RN'_{gateway}\}$ and $\{C_u, RN_{sensor}\}$.

Session key establishment: After verifying for each other, a session key between user and Gateway node can be built.

Password-change part: User needs to enter his previous ID_u and Pw_u, then the smart card computes the new PPW_u and M_u*, matches the M_u* with M_u. If not, the new password change request will be rejected. Otherwise, it would be accepted, then, the user input his new password.

Drawbacks of Park and others' scheme: We find two weaknesses of Park and Others schemes after analyzing the process of their protocols.

We assume that Eve was an intruder who can control the communication between the user, the Gateway and the sensor node. Eve has abilities of eavesdropping, altering and intercepting the wireless messages at any time. Alice is a legal user.

Impersonating attack: Supposing that previous login messages (DID_u, T, ID_u, RN_u) of Alice has been intercepted by Eve. Eve does not know anything about Alice's password or identity but Eve could simply impersonate Alice to access the WSNs. The details of the impersonating attack are shown as follows:

Step 1: Eve→Gateway node: (DID_u, T', ID_u, RN_u)

Step 2: The Gateway node checks the timestamp as $(T1\text{-}T')<\Delta T$ after receiving the login request from the user. Supposing that T' is valid $K_u^* = h(x_a \| ID_u)$, $h(ID_u \| PPW_u^*) = DID_u \oplus h(K_u^* \| T)$, $A_u = h)h(ID_u \| PPW_u)^* \| K_u^* \| RN_u)$ will be calculated by the Gateway node. Then, it responds to Eve with $\{A_u, RN_{gateway}\}$

The impersonating attack was proved to be successful by performing the above steps. Eve's login request was accepted and Eve can easily imitate any user to login into the Gateway at any time.

MITM attack: Assume that Eve is active between the Gateway and the sensors. And Eve can intercept the Gateway node message $\{DID_u, T_2, RN'_{gateway}\}$ and simply alter the request to be (DID_u, T', ID_u, RN_u) by delete the original T' and $RN'_{gateway}$ where, T' is a current timestamp and $RN'_{gateway}$ is a random nonce of Eve. Eve transmits the altered request to the sensor node around him. The sensor node will receive the request from Eve, the details is shown as following:

Step 1: The sensor node verifies the timestamp $(T^*-T_2)>\Delta T$. While T^* is valid, the sensor would calculate $C_u = h(Z_n \| T_2 \| RN_{gateway})$ and create RN'_{sensor}. Here, the sensor knows nothing about the request which he receives, he considers the request as a legal one and responds to Eve

Step 2: Sensor→Eve: (C_u, RN'_{sensor}). Eve could also replace C_u with C'_u after receiving the message from the sensor. Then, Eve transmits the altered authentication message to the sensor

Step 3: Eve→Sensor: It is obvious that the sensor will reject the request for $C_u \neq C_u'$

It is seemingly that this protocol rejects Eve but the detection of the MITM attack is too late. Eve can easily make the sensor node out of energy by numerous of attempting verification.

Certainly, Park and others' protocol has overcome the drawbacks of (Das, 2009; Chen and Shih, 2010; Yoon and Yoo, 2011) but failed to the impersonating attack and MITM attack. However, there are still impacts on real-time WSNs by our analysis. To solve the problem in (Ko, 2008; Lee, 2008; Chen and Shih, 2010; He *et al*., 2010; Khan and Alghathbar, 2010; Yoo *et al*., 2012) we propose a secure and efficient mutual user authentication protocol named MUAP which provides the necessary security and efficient services to WSNs at a reasonable computation and communication consumption in next section.

PROPOSED MUTUAL USER AUTHENTICATION PROTOCOL MUAP

A special type of cryptography named Shamir secret sharing algorithm was used in this protocol. First, let us review the Shamir secret sharing algorithm (Dolev *et al*., 2011; Ulutas *et al*., 2011; Aldosary and Howells, 2012; Coron *et al*., 2013). Generally, Shamir (k, n) secret sharing algorithm divides a secret s into n parts called child-secret, the secret S can be recovered if only the number of the child-secret is equal to k, or more.

A secret $S \in GF(q)$ (that is, q is a large prime number, GF(q) is in Galois field) will be divided into n parts by this polynomial $f(x) = a_0+a_1x+a_2x^2+...+a_{k-1}x^{k-1} \bmod q$. Each of the parts has its unique identifier $x_1, x_2,... ..x_n \in GF(q)$, $a_1, a_2... a_{k-1} \in GF(q)$ and $a_0 = S$. Then, all parts of the secret will be gotten as $f(x_1), f(x_2)... f(x_n)$. Finally, distribute the $\{xi, f(x_i)\}$ (that is i = 1,2... n)) as a key to each participant. In MUAP, we distribute $\{x_i, f(x_i)\}$ to each legal user as his identity number. The identity number will be used at process of authentication.

We consider a WSN which consists of two kinds of devices those are low-resource devices and high-resource devices. The high-resource devices, like Gateway nodes, can resist the tampering attacks but the low-resource devices cannot. User can access to the WSN and get the sensor data by using their terminal equipment like smart phone, or laptop. Certainly, before that, user must register to the Gateway node and get the permission.

To introduce MUAP protocol, we make the following assumptions. And the notations used in this study are shown in Table 1.

Table 1: Symbols used in MUAP

Symbol	Description
ID_u, PW_u	Identity and password of the user
ZUC, $EEA3_k$	Encryption and decryption algorithm, k is a key
f(.)	A function to generate a sharing
S	A secret
b	A random number
ID_{sensor}, $ID_{gateway}$	The identity of sensor and gateway node

- The Gateway is absolute safe and never compromised, also it is a high-power device
- A periodic secret key is maintained by Gateway and sensor to encrypt communication data in authentication process
- The Gateway and sensor hold the same the initial key of ZUC (Liu *et al*., 2010; Zhou *et al*., 2011; Sekar, 2012) which is a lightweight stream encryption algorithm. All the authentication data will be encrypted by the stream encryption algorithm

The MUAP protocol consists of three parts: Registration part, authentication part and password-change part.

Registration part: In order to access the sensor data, each user has to register himself with by passing their ID_u and $PPW_u = h(PW_u) \oplus b$ to the Gateway node in a secure channel. After receiving these two messages, the Gateway node will choose S and use the Shamir secret sharing algorithm to calculate the $f(ID_u)$, then performs the following steps: The Gateway will call the ZUC algorithm to generate the key K_1 whose length is the same as $ID_u \| h(f(ID_u)) \oplus ID_{gateway}$ to encrypt it. Then, calculate $A_u = EEA_{3K1}[ID_u \| h(f(ID_u)) \oplus ID_{gateway}]$. S the Gateway chooses is a periodical-change parameter, so each user must reregister to the Gateway node after S changes.

After that, user will get a smartcard with the following parameters: $\{A_u, B_u, h[f(ID_u)]\}$. Then, user needs to add the random number b to the smartcard. Now, the register part is done.

Authentication part: The procedures of the authentication part in MUAP are shown in Fig. 2. This part consists of three sub-phases: Login phase verification phase and session key establishment.

Login phase: The user needs to insert his smartcard into the terminal and input ID_u and PW_u when he wants to access the sensor data. The smartcard will check the user identity after receiving the login request. Then the smartcard will calculate $B_u^* = h[ID_u \| h(f(ID_u)) \oplus h(b \oplus PW_u)]$ and judges if($B_u == B_u^*$), if yes, proceeds to next step: Calculate $C_u = h(B_u \oplus T')$, then transmit the message (that is $\{C_u, A_u, T'\}$) to Gateway, T' is the current system timestamp of the user; otherwise, deny the login request.

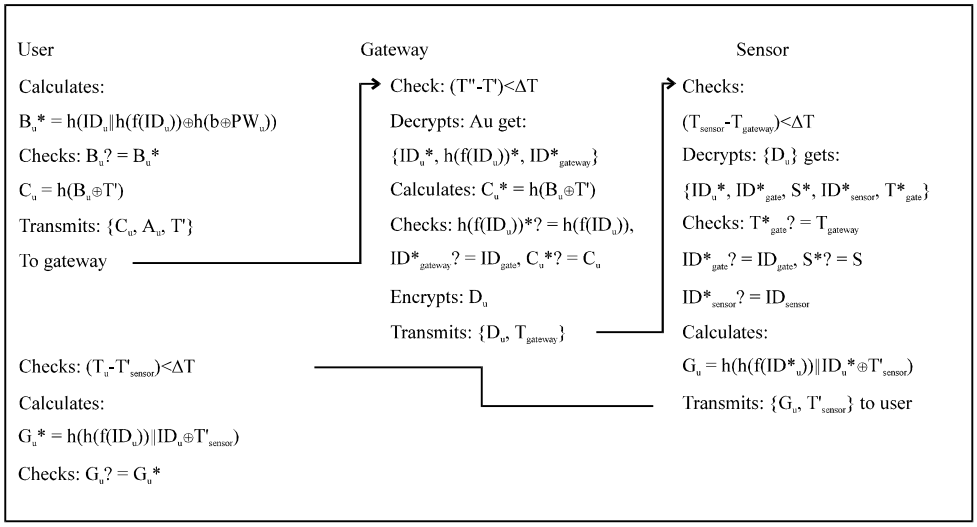

Fig. 2: Authentication part of MUAP protocol

Verification phase: When the Gateway receives the login request from the user, the following steps will be done.

Step 1: Judge (T''-T')<ΔT; if yes, proceeds to next step; otherwise denies the login request. Here, T'' is Gateway's current system timestamp and ΔT is the maximum tolerable interval

Step 2: Gateway decrypts A_u by calling the ZUC algorithm to generate the key K_1, then gets $\{ID_u^*, h(f(ID_u))^*, ID^*_{GateWay}$ and calculates $C_u^* = h(B_u \oplus T')$. And compare $C_u^* = C_u$, $h(f(ID_u))^* = h(f(ID_u))\square$, $ID_{gateway}^* = ID_{gateway}$. If all the compares are yes, the Gateway will regard the user as a legal one and proceeds to next step. Otherwise, denies this procedure

Step 3: The Gateway calls the ZUC algorithm to generate another key K_2 and then calculates $D_u = EEA3_{K2}[ID_u \| ID_{gateway} \| S \| ID_{sensor} \| T_{gateway}]$. Here, T'' is Gateway's current timestamp. The D_u and $T_{gateway}$ are transmitted to the sensor

Step 4: The sensor will check $(T_{sensor}-T_{gateway})<\Delta T$ after receiving D_u and $T_{gateway}$. If yes, proceeds to the next step. Otherwise, denies. Here, T_{swnsor} is the sensor's current timestamp

Step 5: The sensor will call ZUC algorithm to generate K_2.Then sensor will decrypt D_u using K_2 and get $\{ID_u^*, ID_{GateWay}^*, S^*, ID_{sensor}^*, T_{gateway}^*\}$

Step 6: Compares $T_{gateway}^* = T_{gateway}$, $ID_{gateway}^* = ID_{gateway}$, $ID_{sensor}^* = ID_{sensor}$, $S^* = S$. If all the compares are yes, the sensor will regard the Gateway and user as legitimate ones. Then, proceed to next step. Otherwise, denies

Step 7: The sensor calculates $G_u = h(h(f(ID_u^*)) \| ID_u^* \oplus T'_{sensor})$ and sends the message $\{G_u, T'_{sensor}\}$ $\{G_u, T'_{sensor}\}$ to the user

Step 8: The user will check $(T_u-T'_{sensor})<\Delta T$ after receiving G_u and T'_{sensor}. If yes, proceeds to next step. Otherwise, refuse. Here, Tu is the user's current system timestamp

Step 9: The user will use the local $h(f(ID_u))$ and ID_u to calculate G_u^* with received parameter T'_{sensor}. Then, compare $G_u = G_u^*$, if yes, the sensor is legal; otherwise, refuse

Session key establishment: If the step 9 is yes, a session key between user and sensor will be built.

Password-change part: When user needs to change his password, he has to do the following steps:

Step 1: User inserts his smartcard into the terminal and inputs ID_u and PW_u, the smartcard calculates $B_u^* = h(ID_u \| h(b \oplus PW_u \oplus A_u)$. Then, checks $B_u^* = B_u$, if yes, do the next step; otherwise, the procedure will be denied

Step 2: User will be required to input a new password PW_{new}, the smartcard calculate a new B_u, B_u, $B_{new} = h(ID_u \| h(b_{new} \oplus PW_{new}) \oplus A_u)$

Step 3: The B_{new} and b_{new} will be written in the smartcard to take the place of the old ones

ANALYSIS OF MUAP PROTOCOL

In this section, we analyze the security and performance of MUAP protocol and compare it with Park and others' protocols.

Security analysis: Similarly, we assume that Eve was an intruder who could control the wireless channels between user, the Gateway and sensor. Eve has abilities of eavesdropping, altering and intercepting the wireless messages at any time. Alice is a legal user.

Replay attack and message-alternation attack: Eve has three methods to carry out this replay attack by eavesdropping the messages of authentication procedures: (1) Intercepts Alice's login message $\{C_u, A_u, T'\}$ and tries to login by replaying it to the Gateway, (2) Intercepts the message $\{Du, T_{gateway}\}$ which is from the Gateway to sensor and tries to replay it to the sensor, (3) Intercepts the message $\{G_u, T'_{sensor}\}$ which is from the sensor to user and tries to replay it to the user. In (i), Eve replays the message $\{C_u, A_u, T'\}$ to the Gateway. The verification of this replayed message will be failed, because of the maximum tolerable interval $(T''-T')<\Delta T$. Even if Eve modifies T' (T'*,T'*≠T') to make it suitable for $(T''-T')<\Delta T$, unfortunately, Eve also cannot get through the verification due to the $C_u^* \neq C_u$ (that is, $C_u^* = h(B_u \oplus T'^*)$). In (ii), Eve replays the message $\{Du, T_{gateway}\}$ to sensor. Similarly, the verification of the replayed message will be fail because of the maximum tolerable interval $(T_{sensor}-T_{gateway})<\Delta T$. Even if Eve modifies $T_{gateway}$ ($T_{gateway}^*$, $T_{gateway}^* \neq T_{gateway}$) to make it suitable for $(T_{sensor}-T_{gateway})<\Delta T$, unfortunately, Eve also cannot get through the verification due to the $T_{gateway}^* \neq T_{gateway}$. In (iii), Eve replays the message $\{G_u, T'_{sensor}\}$ to user. Likewise, the verification of the replayed message will be fail because of the maximum tolerable interval $(T_{sensor}-T_{gateway})<\Delta T$. Even if Eve modifies T'_{sensor} (T_{sensor}^*, $T_{sensor}^* \neq T_{sensor}$) to make it suitable for $(T_u-T_{sensor})<\Delta T$, unfortunately, Eve also cannot get through the verification due to the $G_u^* \neq G_u$ (that is, $G_u^* = h(h(f(ID_u^*)) \| ID_u^* \oplus T_{sensor}^*)$). Therefore, the MUAP protocol is secure against replay attack and message-alternation attack.

MITM attack: Eve also can carry out the MITM attack by modifying the message $\{D_u, T_{gateway}\}$ from the Gateway to the sensor. (1) D_u is a piece of cipher-text. (2) The real timestamp of the Gateway $T_{gateway}$ is in D_u. Eve has no idea about D_u because he knows nothing about K_2. If Eve modified the timestamp $T_{gateway}$ to $T'_{gateway}$ ($T_{gateway} \neq T'_{gateway}$), Eve will not get through the step 6. So, the MUAP protocol can resist the MITM attack.

User-impersonation attack: If Eve wants to carry out the user-impersonation attack to login in the Gateway, he needs to eavesdrop a legal user's login message $\{C_u, A_u, T'\}$ at the time of T'*. We assume that T'* is available for step 1. But the user-impersonation attack will not succeed when proceed to the step 2. Therefore, the MUAP protocol can resist the user-impersonation attack.

Key-guessing attack: In MUAP protocol, we use ZUC algorithm which is a stream encryption algorithm to encrypt the authentication data. One key is used for only once then a new key will be generated in next procedure to encrypt next procedure data. If someone guesses the current key, it will be useless in next procedure. For instance, someone got the key K_1 in the authentication procedure while the K_1 will be useless because of the new key K_2. So, we can see that key-guessing attack could do nothing about the MUAP protocol.

Gateway-bypass attack: We assume that Eve maybe requests to the sensor directly without getting the Gateway's permission. Eve can fabricate a message of Gateway's request to sensor. But it will be recognized because the communication data between the Gateway and sensor are encrypted. So, the Gateway-bypass attack is useless for MUAP.

Mutual authentication protocol: We know that the MUAP is a mutual authentication scheme from the procedure of MUAP. Firstly, the Gateway will check the user by executing the step 2; Secondly, the Gateway will transmit the authentication data to sensor, the sensor also checks the

Table 2: Security comparison

Types of attacks	S.G. Yoo and K.Y. Park	T.H. Lee	D. He and Y. Gao	T.H. Chen and W.K.	P. Kumar and A. Gurtov	MUAP
Resisting replay attack	Yes	Yes	No	No	Yes	Yes
Resisting message-alternation attack	Yes	No	No	No	Yes	Yes
Resisting MITM attack	No	No	No	No	Yes	Yes
Resisting user-impersonation attack	No	No	No	No	Yes	Yes
Resisting key-guessing attack	No	No	No	No	Yes	Yes
Mutual authentication protocol	No	No	No	No	Yes	Yes

Table 3: Computational consumption comparison

Procedures of the protocol	S.G. Yoo and K.Y. Park	T.H. Lee	D. He and Y. Gao	T.H. Chen and W.K.	P. Kumar and A. Gurtov	MUAP
Registration part						
User	1H	2H	1H	-	1H	1H
Gateway	3H	3H	5H	3H	2H+1B	2H+1S+1Z
Authentication part						
User	5H	4H	4H	1H	5H+2B	3H
Gateway	8H	7H	5H	5H	2H+3B	1H+2Z
Sensor	2H	3H	1H	1H	1H+2B	1H+1Z+1S

H: Times of executing hash function, S: Times of executing Shamir secret sharing algorithm, Z: Times of executing ZUC algorithm, B: Times of executing Block Cipher

Gateway by executing the step 6; At last, sensor will transmit the authentication data to sensor, the user also checks the sensor by executing the step 9. Both of the three members will authenticated each other, so, the MUAP is a mutual protocol between user, Gateway and sensor.

Performance analysis: In this part, we compare the performance of the MUAP to that of (Lee, 2008; Chen and Shih, 2010; He *et al*., 2010; Yoo *et al*., 2012; Kumar *et al*., 2013).

Computational consumption: The major computational consumption of the registration part is in the Gateway while the Gateway is a high-resource device. It can calculate complex operations. The consumption of the user in registration part in (Lee, 2008; Chen and Shih, 2010; He *et al*., 2010; Yoo *et al*., 2012; Kumar *et al*., 2013) is approaching. But it is not the same in authentication part. From Table 3, we know that the consumption of the authentication part in (Lee, 2008; Chen and Shih, 2010; He *et al*., 2010; Yoo *et al*., 2012) are lower than that in (Kumar *et al*., 2013) and MUAP. But, from Table 2, we can see Gao's and Chen's protocols cannot resist all the attacks; Park's scheme can resist the replay attack and message-alternation attack but is not good at resisting MITM attack, user-impersonation attack, key-guessing attack. And Lee's can only resist the replay attack. it is obvious that the security in (Lee, 2008; Chen and Shih, 2010; He *et al*., 2010; Yoo *et al*., 2012) cannot catch up with that in (Kumar *et al*., 2013) and MUAP. We know that those protocol is not suitable for the WSNs' security.

The security in (Kumar *et al*., 2013) and MUAP is the same while the computational consumption is different. Kumar's protocol uses the RC5/Skipjack encryption and decryption algorithm which is block cipher, The MUAP uses the lightweight stream cipher. Stream cipher is lower-consumption than the block cipher. So, the Stream cipher is more suitable for WSN. The total computational consumption of MUAP is only 8H, 4Z and 2S while that in (Kumar *et al*., 2013) is

11H and 8B. Here, the computational consumption of S is lower than B. It is clear that the computation overhead of MUAP is lower than that in (Kumar *et al*., 2013). So, the MUAP protocol is more efficient than the protocol in (Kumar *et al*., 2013) at the same security level.

Communication consumption: From Fig. 1 and 2, we know that those protocols have six times of message-exchanging to complete the whole authentication procedure but in MUAP, we need only three times of message-exchanging with the same length of authentication messages.

CONCLUSION

A secure and lightweight authentication scheme is significant for wireless sensor network. We propose a secure and lightweight mutual user authentication protocol to resist those attacks presented in Table 1 using Shamir secret sharing algorithm, timestamp and a lightweight stream encryption algorithm. The analysis and results show that the MUAP is a secure and lightweight authentication scheme. In addition, the MUAP protocol not only can resist those attacks but has lower consumption of computation and communication at the same security level.

ACKNOWLEDGMENT

This study is supported by the Graduation of Xinjiang Research and Innovation Projects under grant No. XJGRI2013038. The authors would like to thank the anonymous reviewers for their constructive comments that helped to improve the quality of this study.

REFERENCES

Aldosary, S. and G. Howells, 2012. A robust multimodal biometric security system using the polynomial curve technique within Shamir's secret sharing algorithm. Proceedings of the 3rd International Conference on Emerging Security Technologies, September 5-7, 2012, Lisbon, Portugal, pp: 66-69.

Chen, T.H. and W.K. Shih, 2010. A robust mutual authentication protocol for wireless sensor networks. Electron. Telecommun. Res. Inst., 32: 704-712.

Coron, J.S., E. Prouff and T. Roche, 2013. On the Use of Shamir's Secret Sharing against Side-Channel Analysis. In: Smart Card Research and Advanced Applications, Mangard, S. (Ed.). Springer-Verlag, Berlin, Germany, ISBN-13: 9783642372872, pp: 77-90.

Crossbow Technology, 2012. MICA2 wireless measurement system. Crossbow Technology Inc., San Jose, California. http://www.eol.ucar.edu/isf/facilities/isa/internal/CrossBow/DataSheets/mica2.pdf

Das, M.L., 2009. Two-factor user authentication in wireless sensor networks. IEEE Trans. Wireless Commun., 8: 1086-1090.

Das, A.K., 2011. An efficient random key distribution scheme for large-scale distributed sensor networks. Secur. Commun. Networks, 4: 162-180.

Dolev, S., M. Kopeetsky and A. Shamir, 2011. RFID authentication efficient proactive information security within computational security. Theory Comput. Syst., 48: 132-149.

He, D., Y. Gao, S. Chan, C. Chen and J. Bu, 2010. An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc Sensor Wireless Networks, 10: 361-371.

Khan, M.K. and K. Alghathbar, 2010. Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. Sensors, 10: 2450-2459.

Ko, L.C., 2008. A novel dynamic user authentication scheme for wireless sensor networks. Proceedings of the IEEE International Symposium on Wireless Communication Systems, October 21-24, 2008, Reykjavik, Iceland, pp: 608-612.

Kumar, P., A. Gurtov, M. Ylianttila, S.G Lee and H. Lee, 2013. A strong authentication scheme with user privacy for wireless sensor networks. ETRI J., 35: 889-899.

Lee, T.H., 2008. Simple dynamic user authentication protocols for wireless sensor networks. Proceedings of the 2nd International Conference on Sensor Technologies and Applications, August 25-31, 2008, Cap Esterel, France, pp: 657-660.

Liu, Z., L. Zhang, J. Jing and W. Pan, 2010. Efficient pipelined stream cipher ZUC algorithm in FPGA. Proceedings of the 1st International Workshop on ZUC Algorithm, December 2-3, 2010, Beijing, China.

Moteiv Corporation, 2012. Tmote Sky: Datasheet. http://www.eecs.harvard.edu/~konrad/projects/shimmer/references/tmote-sky-datasheet.pdf

Sekar, G., 2012. The Stream Cipher Core of the 3GPP Encryption Standard 128-EEA3: Timing Attacks and Countermeasures. In: Information Security and Cryptology, Wu, C.K., M. Yung and D. Lin (Eds.). Springer, Berlin, Heidelberg, pp: 269-288.

Sun, T., X.J. Yan and Y. Yan, 2013. A chain-type wireless sensor network in greenhouse agriculture. J. Comput., 8: 2366-2373.

Ulutas, M., G. Ulutas and V.V. Nabiyev, 2011. Medical image security and EPR hiding using Shamir's secret sharing scheme. J. Syst. Software, 84: 341-353.

Yoo, S.G., K.Y. Park and J. Kim, 2012. A security-performance-balanced user authentication scheme for wireless sensor networks. Int. J. Distrib. Sensor Networks, Vol. 2012 10.1155/2012/382810

Yoon, E.J. and K.Y. Yoo, 2011. Cryptanalysis of robust mutual authentication protocol for wireless sensor networks. Proceedings of the10th IEEE International Conference on Cognitive Informatics and Cognitive Computing, August 18-20, 2011, Banff, AB., Canada, pp: 392-396.

Zhou, C., X. Feng and D. Lin, 2011. The initialization stage analysis of ZUC v1.5. Proceedings of the 10th International Conference on Cryptography and Network Security, December 10-12, 2011, Sanya, China, pp: 40-53.