2019-1027 IJOI
http: //www.ijoi-online.org/

AN EFFICIENT USER AUTHENTICATICATION SCHEME FOR MULTIPLE ACCESSES SCENARIO IN WSN BASED IN IOT NOTION

Sheng-Kai Yang
[1] Assistant Professor, Department of Information management, Chia Nan University of Pharmacy and Science, Tainan, Taiwan, ROC
patrick@mail.cnu.edu.tw

Chuan-Gang Liu*
[2] Associate Professor, Department of applied informatics and multimedia, Chia Nan University of Pharmacy and Science, Tainan, Taiwan, ROC
*Corresponding author: chgliu@mail.cnu.edu.tw

Tsung-Lin Lee
[3] Professor, Department of Architecture, China University of Science and Technology, Taipei, Taiwan, ROC
tllee58@cc.cust.edu.tw

Abstract

Internet of Things notion is an emerging and popular concept, which is composed of heterogeneous networks. Wireless sensor network plays a vital role in such notion, where the users can directly send control commands and gather sensed data to and from deployed sensors, respectively. Hence, in such network, access security is much more essential and the user authentication scheme is one of popular security topics in WSN. Previous authentication works usually focus on one user to one sensor accessing scenario. However, for future IoT applications, such as smart-home, there are a large number of sensor nodes in WSN architecture, where one user usually wants to control multiple sensor devices in a short time or at the same time. In such network phenomenon, we call it as multiple accesses scenario. Accordingly, this paper proposes an authentication and key agreement scheme which enables a remote user to efficiently complete multiple authentication processes at a time in the multiple accesses scenario. This proposed authentication scheme is suitable for the resource-constrained WSN architecture. Further, our scheme also considers the security flaws of two-factor authentication and designs a stronger security protection. In our security feature and performance evaluation, our proposed scheme achieves several security goals and, meanwhile, ensures the efficiency.

Key Words: Internet of Things, Wireless sensor network, two-factor authentication

Introduction

Internet of Things notion is to construct the global network composed of everything in the world. This global network is composed of the several heterogeneous networks in which wireless sensor network is one critical network consisting of spatially distributed autonomous sensor nodes. The applications in WSN (Akyildiz et al., 2002) cover the wide life fields, including traffic monitor, healthcare monitor, landslide detection, assert tracking, etc. In WSN, access security is much more essential for WSN. If without any security defense, malicious users could disclose secret data and personal privacy easily.

Xue et al. (2013) presents five basic authentication models for WSN. Among them, the fifth model seems to be appropriate for the communication model in IoT environment. Turkanović et al. (2014) also apply this model. Their novel authentication scheme allows one user to access the desired sensor node directly in a secure without the aid of GWN. However, for some applications, like smart-home concept, there are dozens of sensor nodes in WSN architecture and the user may want to control more than one sensor devices in a short time or at the same time. In such network phenomenon, we call it as multiple accesses scenario. According to previous research, in such a circumstance, the authentication sessions should be initiated again and again in a very short time. Some unnecessary security risks will arise and it seems not an efficient authentication manner. In this paper, we propose a new authentication model for multiple accesses scenario. In our authentication model, the user just needs to connect with one of multiple sensor nodes and pass authentication message to it. Then, the chosen sensor node, namely Representative Sensor Node (RSN), delegates authentication task to corresponding GWN. After that, GWN transfers the authentication and key agreement message to other sensor nodes and these sensor nodes can obtain the session key securely. Those sensor nodes send back their keys to GWN and GWN can respond those secure session keys to the User. Via our proposed algorithm, for authentication of multiple accesses, the user just needs to implement authentication and key agreement algorithm once. Hence, our proposed algorithm saves much communication resource and achieves efficient authentication and key agreement process in WSN based on IoT notion.

Literature Review

Recently, Smart-Card based password authentication (i.e. two-factor authentication) schemes catch much attention and many studies develop several related authentication schemes in WSN. Das et al. (2012) proposed a dynamic password-based user authentication scheme which achieves better security and efficiency. Further, they only use the XOR and Hash computations, which is suitable for resource-constrained WSN environment. However, Wang and Wang (2014) demonstrate that it still cannot achieve several security goals and they discover it is vulnerable to smart card security breach attack and privileged

insider attack. Further, they point out the serious defect, the key disclosure. Xue et al. (2013) propose a temporal-credential-based mutual authentication and key agreement scheme, which claims that its scheme can prevent several attacks. However, Wang and Ma (2012) find the scheme proposed in the literature (Xue et al., 2013) has security weaknesses such as inability to resist smart card security breach attack, privileged insider attack and password disclosure. Li et al. (2013) and Turkanovic´ et al. (2013) propose enhanced authentication scheme based on the Xue et al.'s scheme.

Recently, Turkanovic´ et al. (2014) proposes an authentication and key agreement scheme in WSN based on IoT notion. They employ the fifth authentication model described by Xue et al. (2013) to develop their novel authentication scheme. Then, Farash et al. (2015) also proposed an improvement of the Turkanovic´ et al.'s algorithm. Later on, Amin et al. (2016) propose multi-gateway WSN in IoT environment. However, previous authentication model only considers one user to one sensor accessing scenario and in fact, in WSN, one user usually wants to control multiple sensor devices at the same time. Whereby a new authentication and key agreement scheme is proposed.

Proposed scheme

1. One new authentication and key agreement model

This paper proposes a new authentication model composed of four relationship models, such as User-Representative sensor (U-R), Representative sensor-GWN (R-G), GWN-Multi-sensor node (G-M) and GWN-User (G-U) relation models as shown in Figure. 1.

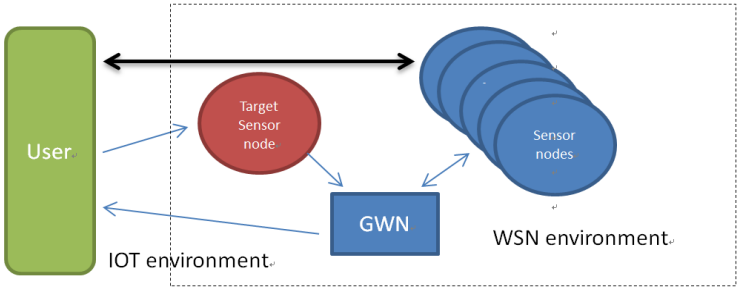

Figure 1. The new authentication model for one bunch of accesses scenario.

2. An efficient authentication and key agreement algorithm

There are five phases in such authentication algorithm, including Pre-deployment, Registration, Login, Authentication, Key Response phases. Table 1 shows the definition of parameters used in the following explanation of this algorithm.

Table 1. Notations used in our proposed authentication algorithm.

Parameters	Definitions
S_j	Sensor node j
U_i	The User
SID_j	The identification of the sensor node j
UPW_i	The user password assigned by the User i
MPK_i	The reformed user password of U_i
RUP_i	A masked identification of U_i
$K_{GWN\text{-}Sj}$	A shared secret key between the GWN and S_j
P_{GWN}	The secret key only owned by GWN
P_{GSj}	The secret key shared by GWN and S_j
ΔT	The valid time interval for transmission delay
UID_i	The identification of the U_i
q_i	A randomly number generated by SC
T_{Ri}	The current timestamp sending message out from the user
T_{Sj}	The current timestamp sending message out from the sensor node
T_{CG}	Current timestamp in GWN
P_{GUi}	Secret key shared by the U_i and GWN
I_{Sj}	The information about S_j in GWN
I_{Ui}	The information about the User i in THE GWN
RSN	Representative Sensor Node
SID_{Sa}	The SID set of these nodes
S_a	The set of all sensor nodes expected to be controlled by the User
K_i	Random nonce key generated by U_i
K_j	Random nonce key generated by S_j
SK_{ij}	The Session Key between the User i and the sensor node j

Pre-deployment Phase

The deployment and pre-definition in WSN are main work items in pre-deployment phase. The service provider should provide Smart Cards with unique UID_i to the users and these $UIDs$ are stored in GWN meanwhile. Each sensor node is defined with SID_j and has a secret key $K_{GWN\text{-}Sj}$ shared with GWN. Initially, GWN stores SID_j, $K_{GWN\text{-}Sj}$ for sensor node j and UID_i for the User i. The User should randomly select one of sensor node in WSN to be the RSN. While the User i wants to access WSN, the user firstly registers with GWN and so does the Representative Sensor Node. The registration phase is as follows.

Registration Phase

The registration process between the GWN and the User i is called as U-G registration phase. The procedure of this sub-phase is depicted in Figure 2. The full details of this phase are as follows.

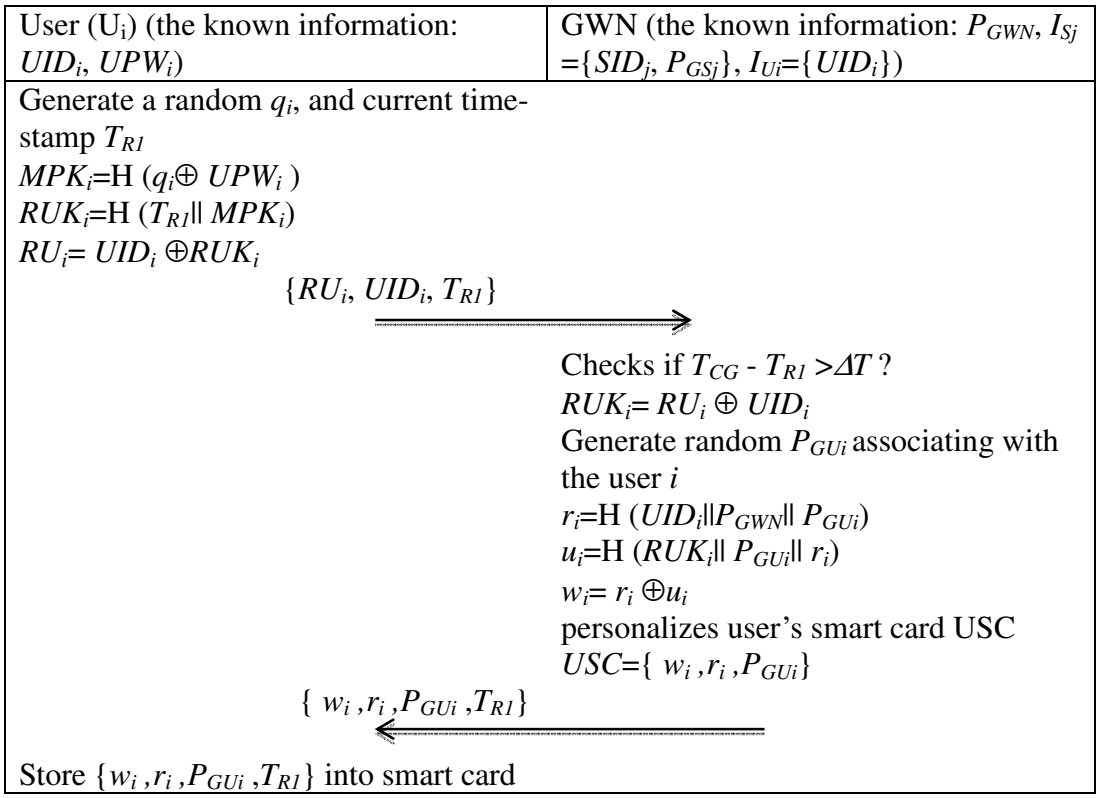

Figure 2. U-G registration procedure.

Step 1: In the user end, User i prepares four parameters, UID_i, UPW_i , q_i and the current timestamp T_{R1}, to initiate the registration phase.

Step 2: The User i computes a modified password, MPK_i = H ($q_i \oplus UPW_i$)..

Step 3: The user computes masked password RUK_i=H (T_{R1}|| MPK_i).

Step 4: The user obtains RU_i via XORing UID_i and RUK_i. Then the user sends RU_i, RUP_i ,T_{R1} to the *GWN* via a secure channel.

Step 5: On receipt of message from the User i, the GWN checks if T_{CG} - T_{R1} >ΔT. If it holds, the GWN rejects this registration message and the authentication process ends.

Step 6: The GWN computes RUK_i = $RU_i \oplus UID_i$. And then it also generates random secret key associating with the User i, P_{GUi}.

Step 7: With UID_i, P_{GWN} and P_{GUi}, the GWN computes r_i=H (UID_i||P_{GWN}|| P_{GUi}) and u_i=H (RUK_i|| P_{GUi}|| r_i).

Step 8: After obtaining r_i and u_i, the GWN computes w_i= $r_i \oplus u_i$.

Step 9: The GWN personalizes the user's smart card with the parameter set {w_i , r_i , P_{GUi} ,T_{R1}} and then sends it to the User i.

Step 10: The user stores { w_i , r_i , P_{GUi}, T_{R1} } into smart card in the end of this phase.

After the U-G registration phase, the user uses MPK_i instead of UPW_i thereafter.

The procedure of t S-G registration phase is depicted in Figure 3. The following steps explain the details of this phase.

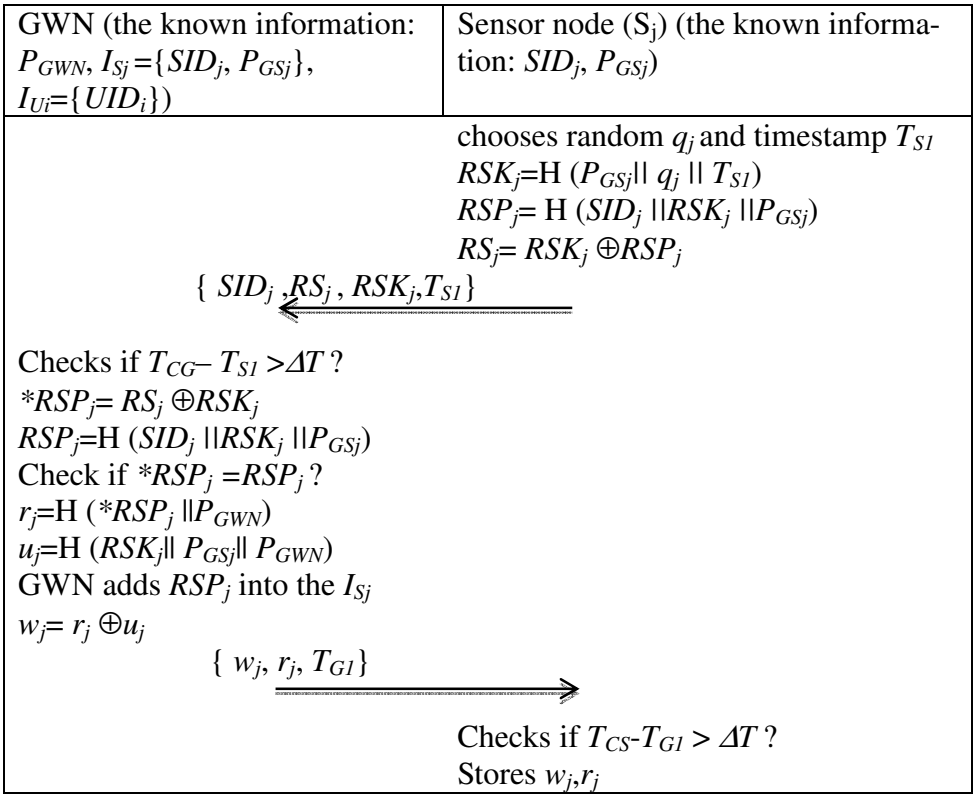

Figure 3. S-G registration procedure.

Step 1: At the beginning, the sensor node j prepares random value q_j and the timestamp T_{S1}.

Step 2: The sensor node j computes the masked shared secret key, RSK_j= H (P_{GSj} || q_j || T_{S1}), with the use of P_{GSj}, q_j, T_{S1} .

Step 3: Similar to above step, the sensor node j computes RSP_j= H (SID_j ||RSK_j ||P_{GSj}), with the use of SID_j, RSK_j, P_{GSj}.

Step 4: The sensor node j computes RS_j= RSK_j ⊕RSP_j. After these initial computations, the sensor node j sends the parameter set {SID_j , RS_j , RSK_j, T_{S1}} to the GWN.

Step 5: Upon receiving parameters from the sensor node j, the GWN checks if T_{CG}– T_{S1} >ΔT. Then GWN computes *RSP_j with the use of RS_j , RSK_j. (Note: the * sign in the front of the notation denotes this notation is candidate notation needed to be verified).

Step 6: With the use of SID_j, RSK_j and P_{GSj}, the GWN computes another RSP_j. The result of comparison between both RSP_j determines the validation of this registration message. If

both RSP_j are different, this registration terminates.

Step 7: The GWN computes r_j =H (*RSP_j || P_{GWN}) and u_j =H (RSK_j || P_{GSj} || P_{GWN}).

Step 8: The GWN adds RSP_j into the I_{Sj} and then computes $w_j = r_j \oplus u_j$. Then, the GWN sends information set $\{w_j, r_j, T_{G1}\}$ to S_j .

Step10: On receipt of information set $\{ w_j, r_j, T_{G1}\}$, the sensor node j checks if T_{CS}-$T_{G1} > \Delta T$. If no, the sensor node stores w_j, r_j or it rejects this message.

Login Phase

In Login Phase, the user randomly chooses a Representative Sensor Node (*RSN*) in S_a and tries to login it. Figure. 4 shows U-S login procedure. The details of this phase are as follows.

User (U_i) (the known information: UID_i, MPK_i)	RSN (S_j) (the known information: SID_j, P_{GSj} ,w_j,r_j)
SC login Input password MPK_i *RUK_i=H (T_{R1}|| MPK_i) *u_i=H (*RUK_i|| P_{GUi}|| r_i) *w_i= $r_i \oplus$*u_i Check if *w_i =w_i ? RUP_i=H (T_{R2}|| UID_i) M_i=H (u_i|| P_{GUi} || T_{R2}|| r_i) Select random nonce K_i D_i= $K_i \oplus M_i$ Choose the RSN from S_a, and SID_{Sa} denotes the SID set of S_a. { RUP_i ,w_i, D_i , M_i ,T_{R2}, SID_{Sa} } ⟹	
	Checks if T_{CS}- T_{R2}> ΔT ?

Figure 4. User-sensor login procedure.

Step 1: The user inserts his/her smart card into the terminal and enters reformed password MPK_i.

Step 2: The terminal exploits T_{R1} and MPK_i to compute *RUK_i=H (T_{R1}|| MPK_i) and then it employs the secret information in smart card, { r_i ,P_{GUi} }, to compute *u_i =H (RUK_i || P_{GUi} || r_i).

Step 3: After computing u_i, the terminal computes* w_i= $r_i \oplus$*u_i.

Step 4: The terminal checks if computed $*w_i$ is equal to w_i stored in smart card and if the result holds, go to next Step, or this login process is terminated.

Step 5: The terminal computes a masked *UID*, RUP_i=H (T_{R2}|| UID_i).

Step 6: The terminal computes M_i =H (u_i|| P_{GUi} || T_{R2}|| r_i) with the use of (u_i, P_{GUi}, T_{R2}, r_i).

Step 7: The terminal chooses random nonce K_i and computes D_i with the use of K_i , M_i.

Step 8: The terminal sends the parameter set {RUP_i ,w_i, D_i , M_i ,T_{R2}, SID_{Sa} } to RSN. SID_{Sa} denotes the *SID* sequence in S_a. The first one in SID_{Sa} is *SID* of the RSN.

Step 9: The RSN receives the login message and checks if T_{CS}- T_{R2}> ΔT. If the inequality holds, the RSN rejects this login request.

Authentication Phase

This phase can be divided into RSN-GWN authentication phase and GWN-MSN authentication phase. Figure 5 shows RSN-GWN procedure.

The RSN (S_j) (the known information: SID_j, P_{GSj} ,w_j,r_j)	GWN (the known information: P_{GWN}, I_{Sj} ={SID_j, RSP_j, P_{GSj} }, I_{Ui}={ P_{GUi} , UID_i})
$u_j = w_j \oplus r_j$ L_j=H (P_{GSj}|| T_{R2}|| T_{S2}||SID_j) $\oplus$ u_j { RUP_i, w_i, D_i, M_i , T_{R2}, T_{S2}, w_j, L_j, SID_{Sa} } ⟹	
	Checks if T_{CG}– T_{S2} >ΔT ? r_j=H (RSP_j ||P_{GWN}) $*u_j = w_j \oplus r_j$ u_j= L_j $\oplus$H (P_{GSj}|| T_{R2}|| T_{S2}||SID_j) checks if $*u_j = u_j$? *For each UID do* $*RUP_i$=H (T_{R2}|| UID_i) Checks if any $*RUP_i = RUP_i$? if yes, continue process ,or authentication fails. r_i=H (UID_i||P_{GWN}|| P_{GUi}) $*u_i = w_i \oplus r_i$ $*M_i$=H ($*u_i$|| P_{GUi} || T_{R2}|| r_i) check if $*M_i = M_i$? K_i=D_i $\oplus$$*M_i$

Figure 5. RSN-GWN authentication procedure.

RSN-GWN authentication sub-phase

Step 1: RSN computes u_j, using the formula as defined previously, i.e. u_j =w$_j$ ⊕ r_j.

Step 2: Then, it conducts L_j, i.e. L_j =H (P_{GSj}|| T_{R2}|| T_{S2}||SID_j) ⊕ u_j.

Step 3: The sensor node sends { RUP_i, w_i, D_i, M_i , T_{R2}, T_{S2}, w_j, L_j, SID_{Sa} } to GWN.

Step 4: On receipt of authentication message from the RSN, GWN checks if T_{CG}− T_{S2} <ΔT. If the inequality holds, the GWN computes r_j = H (RSP_j ||P_{GWN}) or this authentication process terminates.

Step 5: The candidate *u_j= w_j ⊕ r_j, hence, can be obtained with the use of w_j , r_j.

Step 6: GWN can also compute u_j = L_j ⊕H (P_{GSj}|| T_{R2}|| T_{S2}||SID_j). Then, GWN compares both u_j and if they are the same, mutual authentication between sensor node and GWN is successful. Or this authentication process terminates.

Step 7: In order to verify the validation of received RUP_i, the GWN computes *RUP_i =H (T_{R1}|| UID_i) with each UIDs in its databse. If there is no adequate UID for this received RUP_i, the GWN reject this registration message and the authentication process ends.

Step 8: GWN computes r_i = H (UID_i ||P_{GWN}|| P_{GUi}).

Step 9: GWN computes *u_i = w_i ⊕ r_i.

Step 10: GWN computes *M_i= H (*u_i|| P_{GUi} || T_{R2}|| r_i) with the use of *u_i, P_{GUi}, T_{R2}, r_i.

Step 11: GWN checks if * M_i is equal to received M_i. If not, this authentication process terminates, or GWN computes K_i with use of received D_i and *M_i.

After verifying authentication message between RSN-GWN, GWN can retrieve the session key K_i and then sends it to all sensor nodes in S_a. Each sensor node j receives the session key K_i and then the session key pairs (K_i, K_j). Each sensor node sends the session key pair (K_i, K_j) back to the user via GWN. Figure 6 shows this authentication GWN-MSN e procedure.

GWN-MSN authentication sub-phase

Step 1: For each sensor node S_j in S_a, GWN should run the following steps.

Step 2: GWN computes OSP_j and OSK$_j$ with the formulas, OSP_j =H (r_j||SID_j|| T_{G3}||T_{S2}|| T_{R2}) and OSK$_j$ =H (r_j|| P_{GSj} || T_{G3}||T_{S2}|| T_{R2}).

Step 3: Then, GWN computes OS_j =OSP_j ⊕ OSK_j.

Step 4: GWN hides the user's key, K_i, in GC_{ij} =H (OSP_j || TG3||TS2|| TR2) ⊕ K_i.

Step 5: After the above four steps, GWN sends { OS_j, T_{G3}, T_{S2}, T_{R2}, OSK_j, GC_{ij} } to each sensor node, S_j.

Step 6: In sensor node S_j's end, it checks if T_{CS}- T_{G3}>ΔT once it receives the messages from GWN. If inequality holds, the authentication and key agreement process terminates, or S_j computes *OSP_j.

Step 7: S_j computes another OSP_j with the use of its known information and the received message.

Step 8: S_j checks if *OSP_j is equal to OSP_j. If it is true, S_j can obtain the user's

key, $K_i = GC_{ij} \oplus H (OSP_j || T_{G3} || T_{S2} || T_{R2})$. Or, this process terminates.

Step 10: S_j chooses a random nonce K_j to be its key. By the combination of both keys, the session key pair, SK_{ij}, is generated.

Step 11: S_j hides its key K_j in OC_{ij}, where OC_{ij}=H (H (r_j) || T_{G3}||T_{S2}|| T_{R2}|| T_{S3}) $\oplus K_j$. Then it sends { OC_{ij}, T_{G3}, T_{S2}, T_{R2},T_{S3}, OSP_j } to GWN.

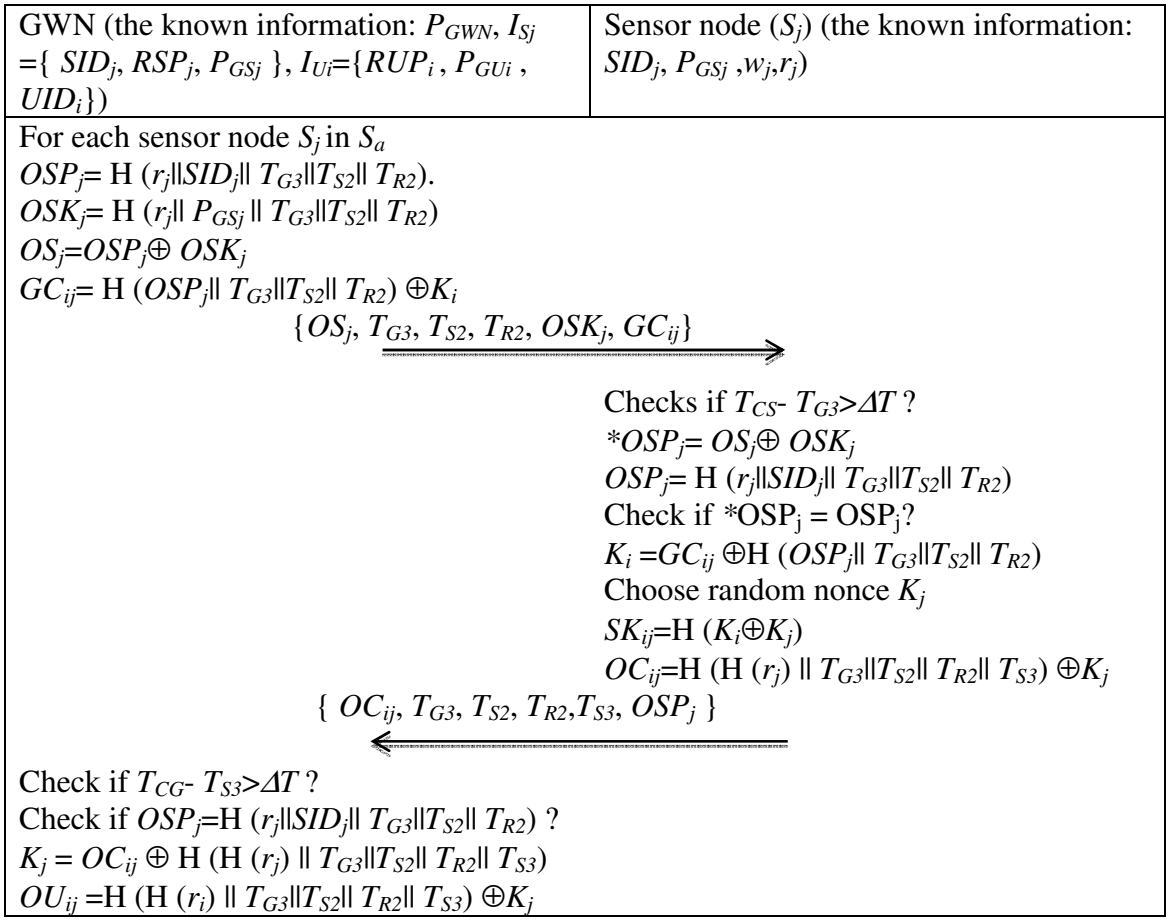

Figure 6. GWN-MSN authentication procedure.

Step 11: S_j hides its key K_j in OC_{ij}, where OC_{ij}=H (H (r_j) || T_{G3}||T_{S2}|| T_{R2}|| T_{S3}) $\oplus K_j$. Then it sends { OC_{ij}, T_{G3}, T_{S2}, T_{R2},T_{S3}, OSP_j } to GWN.

Step 12: GWN checks if T_{CG}- T_{S3}>ΔT, then if inequality holds, this process terminates, or continues next step.

Step 13: GWN checks if OSP_j is equal to H (r_j||SID_j|| T_{G3}||T_{S2}|| T_{R2}) for S_j in S_a. If the inequality holds, this process terminates, or continues next step.

Step 14: GWN recovers the key, K_j, via XORing OC_{ij} and H (H (r_j) || T_{G3}||T_{S2}|| T_{R2}|| T_{S3}).

Step 15: GWN hides the corresponding key of S_j in OU_{ij}, where OU_{ij} =H (H (r_i) || T_{G3}||T_{S2}|| T_{R2}|| T_{S3}) ⊕K_j.

Key Response Phase

Until now, each session key pair has been conducted by each sensor node in S_a and then, GWN sends back the corresponding key of the sensor nodes in S_a to the User. Figure 7 shows this procedure.

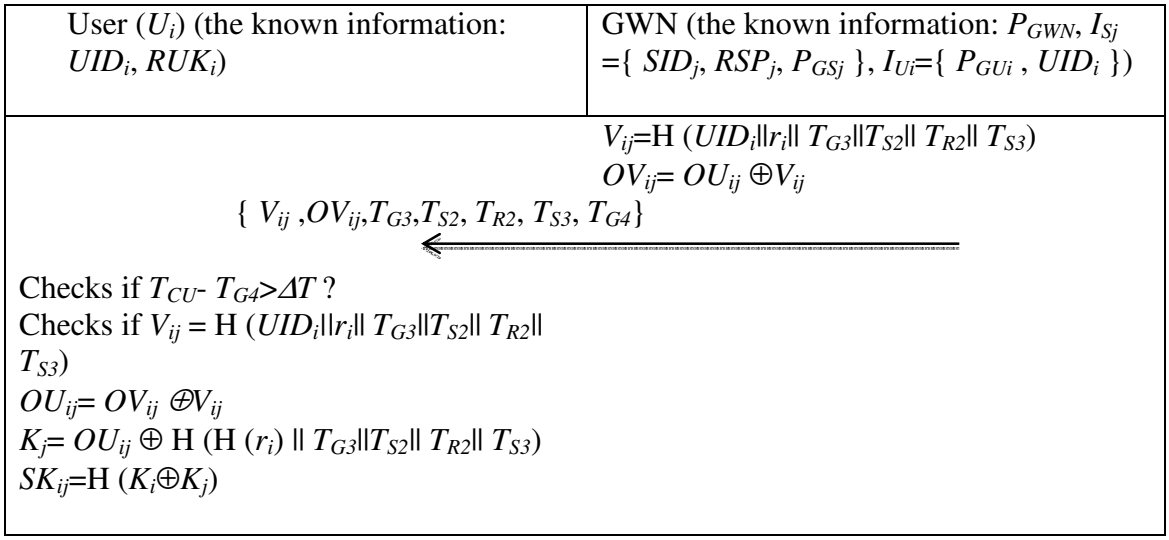

Figure 7. The procedure of Key Response Phase.

Step 1: For assurance of legitimacy of the user, GWN computes V_{ij}, containing the user information UID_i and r_i, for verification.

Step 2: GWN computes OV_{ij} which contains the S_j's key and the validation information, V_{ij}. Then GWN sends {V_{ij} ,OU_{ij},T_{G3},T_{S2}, T_{R2}, T_{S3}, T_{G4}} to the User.

Step 3: On receipt of the authentication message, the User checks if T_{CU}- T_{G4}>ΔT and if inequality holds, the process terminates, or continues next step.

Step 4: The User checks if V_{ij} is equal to H (UID_i||r_i|| T_{G3}||T_{S2}|| T_{R2}|| T_{S3}) with the use of its smart card information. If it is true, the user has verified V_{ij}.

Step 5: The user gets OU_{ij} via XORing OV_{ij} and V_{ij}.

Step 6: The user recovers the key of a sensor node in S_a with the formula K_j= OU_{ij} ⊕ H (H (r_i) || T_{G3}||T_{S2}|| T_{R2}|| T_{S3}).

Step 7: Finally, the user obtains the session key pair (K_i, K_j) and computes the session key, SK_{ij}=H (K_i⊕K_j).

Finally, the user and sensor node, S_j, in S_a have the session keys {SK_{ij}}. The communication between them, therefore, is secure.

Security and performance analysis

Our proposed scheme can support the following features:

1. Secure key agreement: The user's key, K_i, and K_j, are all transferred by secure authentication process.

2. Mutual authentication: In our protocol, each message delivery should be veri-

fied its legitimacy through authentication message.

3. Strong password protection: With the use of MPK_i=H ($q_i \oplus UPW_i$). Thereafter, this modified password substitutes for the weak password..

4. User anonymity: For ID protection, in our proposed protocol, the user uses masked ID, namely RUP_i=H (T_{R1}|| UID_i), to conceal real *UID* in an open and public environment.

Next we try to evaluate the performance of our proposed authentication and key agreement protocol. Here, we compare our scheme with recent other SC-based scheme. As shown in Table 2, firstly, we can discover recent SC-based schemes support mutual authentication.

The key agreement is also supported in recent years. In order to add sensor node dynamically, the schemes of Das et al., Turkanovic´ et al. and our scheme add this function. Our scheme can resist weak-password-based attacks. Table 2 shows the result of this metrics comparison. For the first security metrics, our scheme uses randomly-reformed password and ID to verify the legitimacy of the user and hence can resist the all attacks arising from this security metric and our scheme outperforms other schemes. Next, our scheme can resist reply attack and most schemes can resist this attack, except to Yeh's scheme (2011).

For Stolen-verifier and privileged insider attacks, our scheme does not use password table and we also reform our weak password. Hence, our scheme can resist this attack. For Denial-of-service attacks, our propose scheme, the schemes of Turkanovic´ et al. (2014), Das et al. (2012) can resist it. For the fifth security metric, the schemes of Turkanovic´ et al., Xue et al (2013).,Yeh et al. (2011) and our schemes can resist GWN bypassing attacks. The schemes of Das et al. (2012) do not resist this attack. In our scheme, authentication message must be handled by GWN and transmitted to all other sensors and the user. Hence, the malicious user cannot use GWN bypassing attack to intrude our scheme. Further, GWN in our scheme just uses $14T_h/k$ to complete k authentication requests. Hence, for one user to multiple sensor nodes accessing scenario, our scheme outperforms than other schemes.

Conclusions

In this paper, we try to propose a new authentication and key agreement scheme in WSN based on IoT. We propose a hybrid authentication model suitable to one user to multiple sensor nodes accesses scenario. Further, we also adopt the suggestions of previous study to design strong password protection, which enables our scheme against various attacks arising from weak password. Beside, our scheme also achieves several securities feature, such as mutual authentication, secure key agreement, and password protection. We give a cryptanalysis of our scheme to show the robust of our authentication and key agreement scheme.

Acknowledgements

This paper was supported by the Ministry of Science and Technology of Taiwan under Grant MOST 104-2221-E-041-007 and MOST 106-2221-E-041-003.

Table 2. the security metrics comparison among the proposed scheme and other related schemes

	Items	Yeh et al. (2011)	Das et al. (2012)	Xue et al. (2013)	Turka-novic´ et al. (2014)	Our proposed scheme
Security Feature	Mutual authentica-tion	Yes	Yes	Yes	Yes	Yes
	Key agreement	Yes	Yes	Yes	Yes	Yes
	Dynamical node addi-tion	-	Yes	-	Yes	Yes
	Password change	No	Yes	Yes	Yes	Yes
Security metrics	Weak-Password-based se-curity met-rics (5 items)	No	No	No	No	Yes
	Reply at-tack	No	Yes	Yes	Yes	Yes
	Stolen-verifier and privi-leged in-sider at-tacks	Yes	-	Yes	Yes	Yes
	Denial-of-service attacks	-	Yes	-	Yes	Yes
	GWN by-passing attacks	Yes	-	Yes	Yes	Yes

Weak-Password-based security metric: Impersonation attacks, Many logged-in users with the same login-id attacks, Stolen smart card attacks and smart card breach attacks, Password change attack

References

Akyildiz I. F., Su W., Sankarasubrama-niam Y., Cayirci E. (2002). Wireless sensor networks: a survey, Computer Networks 38, 393–422.

Das A.K., Sharma P., Chatterjee S., Sing J.K. (2012). A dynamic password-based user authentication scheme for hierarchical wireless sensor networks, Journal of Computer Networks 35, 1646–1656.

Farash M. S., Turkanovic´M., Kumari S., Holbl M. (2015). An efficient uer authentication and key agreement scheme for heterogeneous wireless sensor tailored for the Internet of Thing environment, Ad hoc Networks 36, 152-176.

Kumar P., Lee H. (2011). Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks, IEEE Wireless Advanced, London.

Lee C. C., Li C. T., Chen S. D. (2011). Two attacks on a two-factor use authentication in wireless sensor networks, Parallel Processing Letters 21, 21–26.

Li C. T., Weng C. Y., Lee C. C. (2013). An advanced temporal credential based security scheme with mutual authentication and key agreement for wireless sensor networks, Sensors 13, 9589–9603.

Amin R., Biswas G. P. (2016). A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks, *Ad Hoc Networks* 36, 58-80.

Sun D., Li J., Feng Z., Cao Z., Xu G. (2013). On the security and improvement of a two-factor user authentication scheme in wireless sensor networks, Personal Ubiquitous Computing 17, 895–905.

Turkanovic´M., Brumen B., Hölbl M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Networks 20, 96–112.

Turkanovic´M. , Hölbl M. (2013). Notes on a temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, Wireless Personal Communications 77, 1–16.

Wang D., Ma C. G. (2012). On the (in)security of some Smart-card-based Password Authentication Schemes for WSN. Published in IACR Cryptology ePrint Archive.

Wang D., Wang P. (2014). Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks, Ad Hoc Networks 20, 1–15.

Xue, K., Ma, C., Hong, P., Ding, R. (2013). A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, Journal of Computer Networks 36, 316–323.

Yuan J., Jiang C., Jiang Z. (2010). A biometric-based user authentication for wireless sensor networks, Wuhan University Journal of Natural Sciences 15, 272–276.

Yang G. M., Wong D. S., Wang H. X., Deng X. T. (2008). Two-factor mutual authentication based on smart cards and passwords, Journal of Computer System Science 74, 1160–1172.

Yeh H., Chen T., Liu P., Kim T., Wei H. (2011). A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors 11, 4767–4779.