Password based Secure Authentication Methodology for Wireless Sensor Network

Gul N. Khan and M. Zulfiker Ali
Department of Electrical and Computer Engineering, Ryerson University,
350 Victoria Street, Toronto, ON M5B2K3, Canada

Keywords: Authentication Protocol, Secure Authentication, Sensor Data Security, Wireless Sensor Network.

Abstract: Wireless Sensor Network (WSN) is a promising solution for next generation real-time monitoring applications due to its ubiquitous nature, ease of deployment and wide range of applications. The main requirements of a secure WSN architecture are confidentiality, integrity and authentication. User Authentication for wireless sensor networks is a fundamental issue in designing secure WSN systems, where legitimate users are allowed to login and access data from the sensor and gateway nodes. A large number of dynamic strong password and two-factor authentication solutions have been proposed. However, all of these protocols rely on network synchronization and suffer from replay and many logged in users with same login ID threats. We present a secure authentication protocol that avoids replay and multiple login attacks. Our scheme eliminates the need for network synchronization. The scheme is analysed and evaluated for various attacks using SystemC and it provides enhanced security for no extra computing at sensor nodes.

1 INTRODUCTION

Wireless Sensor Networks (WSNs) are used to collect and process environmental data such as temperature, humidity, light, seismic activities, images, etc. WSNs have attracted many researchers due to their ubiquitous nature, easy deployment and a wide range of applications. Wireless networks with thousands of tiny sensors having low processing capabilities and limited memory play an important role for economical solutions of some challenging problems including real-time traffic monitoring, building safety, object tracking, wildlife monitoring, etc. In general, most of the queries in WSN applications are issued at the base stations or gateway nodes of the network. However, one can foresee that there are greater needs to access the real-time data within a WSN. For some applications, the collected data is valuable and confidential, while many applications require integrity and confidentiality of the collected data along with the user privacy. Security measures are incorporated to protect the data access and to prevent intruders from gaining the data access. If the data is made available to the user on demand then user authentication must be ensured before allowing its access.

Many WSN related user authentication schemes have been proposed that are suitable for wireless mobile and low-power devices. IEEE standard 802.15.4 (2003) is the most appropriate communication scheme for low power sensor networks. Sastry and Wagner (2004) observed the merits and limitations of security aspects related to WSNs.

A number of researchers have focussed on the user authentication schemes suited to WSNs. Benenson et al., (2004) introduced an *n*-authentication protocol in which the authentication succeeds if the user can successfully authenticate with a subset of *n*-sensors. Benenson et al., (2005) proposed a public key based user authentication protocol with elliptic curve cryptography. Wong et al., (2006) proposed a strong password-based dynamic user authentication scheme. Tseng et al., (2007) pointed out some weaknesses of Wong et al.'s (2006) scheme and proposed an improved dynamic user authentication method to enhance security. Lee (2008) also analyzed this scheme and proposed two simple dynamic user authentication methods. Ko (2008) pointed out that Tseng's et al., (2007) scheme suffers from replay and forgery attacks. Ko's user authentication scheme (2008) also provides mutual authentication. However, Vaidya et

N. Khan G. and Ali M..
Password based Secure Authentication Methodology for Wireless Sensor Network.
DOI: 10.5220/0004307400350041
In *Proceedings of the 3rd International Conference on Pervasive Embedded Computing and Communication Systems* (PECCS-2013), pages 35-41
ISBN: 978-989-8565-43-3

al., (2009) argued that most of these schemes cannot preserve user anonymity. Das (2009) introduced the two-factor authentication concept to resist many logged in users with the same login-ID and stolen-verifier attacks. Khan and Alghathbar (2010) incorporated enhanced security patch into Das's (2009) scheme. Vaidya et al., (2010) pointed out that several security pitfalls still exist in these schemes and proposed an improvement method that results in a high level of robustness and security. Zhou et al., (2011) have proposed a new dynamic user authentication method employing nonce in place of timestamps.

Two-factor user authentication schemes are expensive but password-based authentication can be easily integrated. To the best of our knowledge Vaidya et al.'s scheme (2009) is the latest variant of strong password-based user authentication method. However, the scheme allows data access from sensor nodes without gateway's notice that makes it vulnerable to gateway bypass attacks due to node compromise attack. Moreover, the scheme does not provide mutual authentication between a user device (UD) and the gateway node (GW). All password-based schemes require strict time synchronization, which increases the network overhead and makes them vulnerable to replay attack within a time interval. Their methods do not resist many logged in users with same ID attacks. In this paper, we propose a robust and secure user authentication method that resists gateway bypass, replay and many logged in user with the same ID attacks.

2 AUTHENTICATION SCHEME

The notations used in this paper are listed in Table 1. Our scheme assumes a typical WSN setup shown in Figure 1. Authorized users can access the WSN anywhere in the network with mobile devices by communicating with a sensor node. Before issuing any queries, a user must register at the gateway (GW) node. Upon successful registration, the user can submit its query to a sensor node (SN) any time within a predefined period. The allocation of a secret key to the user and sensor nodes is dynamic that takes place during registration. A flag is maintained for each user in the GW to prevent multiple logins.

We assume that the registration process is carried out in a secure manner and the database stored at the GW node is secure. In our user authentication scheme, we used nonce in place of timestamp that eliminates the need for strict time synchronization. Our scheme has four phases: the registration, login, authentication and password change. The communication flow of our authentication protocol is given in Figure 2.

Table 1: Notations used in the proposed scheme.

$\oplus$	Bit-wise Exclusive-OR operation
$\|\|$	Bit-wise Concatenation
H(d)	Hash function of d
N_0, N_1	Random nonce
PW	Password chosen by user
t, T_i	Current time recorded by a node
TS	Timestamp for particular user
TID	Temporary User ID
UID	User's identity
vpw	SHA-4 of user password
x_s	Secret key known to the GW
X_s	Key generated by GW that is also known to user and sensor nodes.

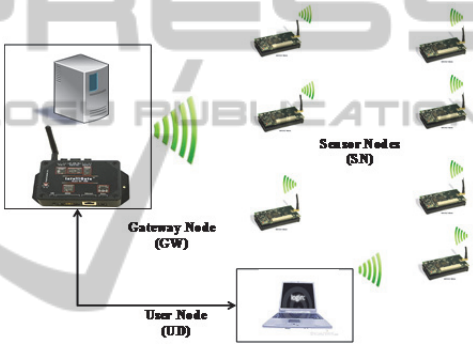

Figure 1: Typical network setup.

2.1 Registration

There are seven steps of the registration phase R1-R7 as given below:

R1: A registration interface is launched by a user's device (UD) who inputs its ID (*UID*) and a chosen password *PW*. The user computes the Hash of *PW* and stores it as *vpw*.

R2: UD submits its identity *UID* and *vpw* to GW node on a secure channel.

R3: GW stores the secret key x_s and generates a random nonce N_0 and computes TID and X_s as shown in Figure 2. Then GW stores (*TID, vpw,* X_s *and TS*) in the user database. The flag value for the user is set to zero.

R4: GW replies the user for a successful registration with *Xs* and random number N_0.

R5: Then UD computes *TID* as shown in Figure 2 and stores *TID* and *Xs* for future use.

R6: GW distributes *(TID,* X_s*, TS)* to those SNs that are able to provide login interface to the user.

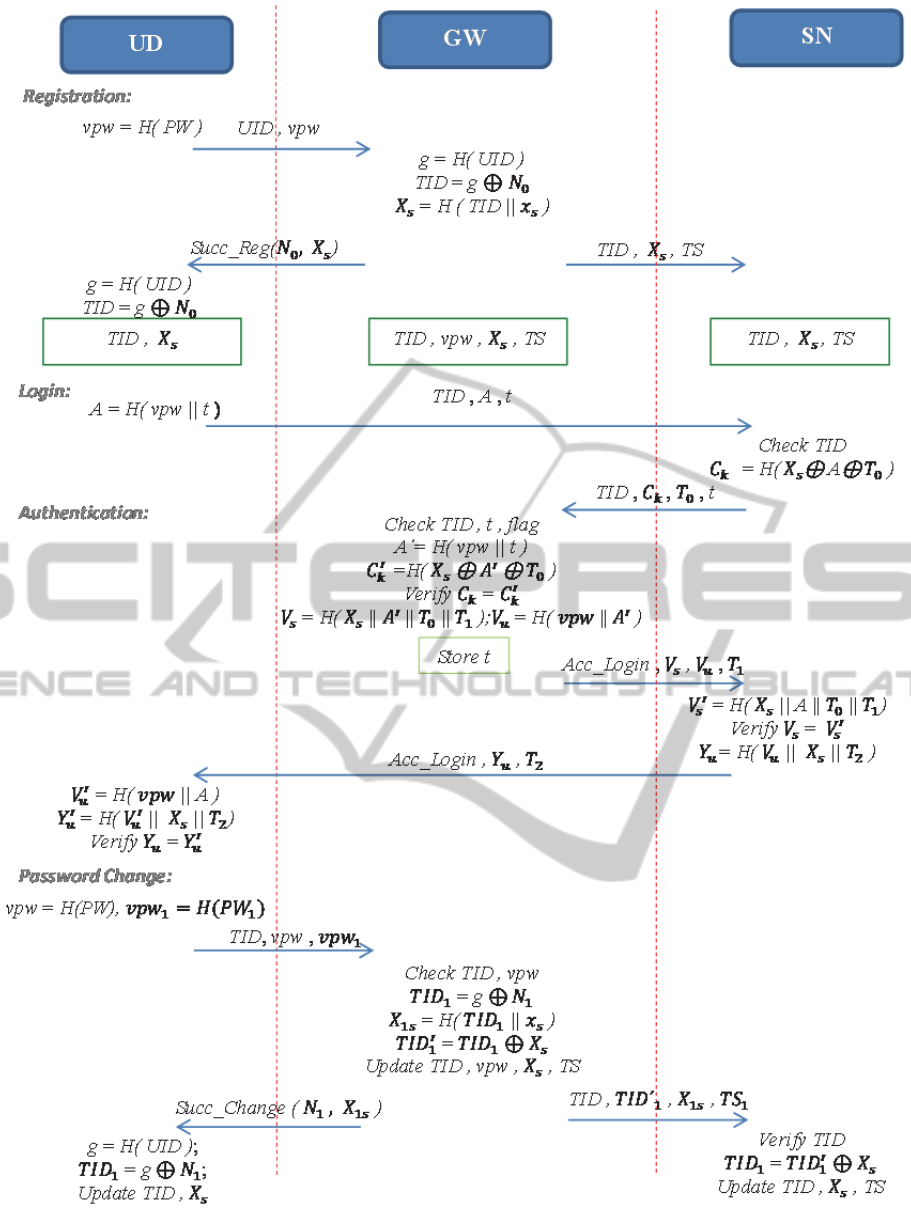

Figure 2: Communication flow of the proposed protocol.

R7: A small database is maintained in the sensor node to store (*TID*, X_S, *TS*) for the user.

2.2 Login Phase

A user needs to login to a sensor node to get sensory information. The main steps of login phase are:

L1: At time *t*, a user initiates login and computes *A*, which is the hash of *vpw* in concatenation with *t*.

L2: The user submits *(TID, A, t)* to a sensor node.

L3: Upon receiving the login request at time T_0, the sensor node checks its database to validate *TID*. On validation, the sensor node (SN) retrieves the corresponding *A* and computes C_k as shown in Figure 2. Otherwise, the login request is rejected.

L4: Sensor node sends *(TID,* C_k, T_0, *t)* to the GW.

2.3 Authentication Phase

For authentication, GW receives (*TID*, C_k, T_0 and *t*) from SN at time T_1. The main steps of this phase are:

A1: GW checks the database whether *TID* is a valid user. If *TID* is not valid then login is declined. Otherwise, the GW checks whether time *t* is

recorded against the *TID* in the database. If *t* is already recorded then login is not allowed that will prevent a replay attack. Otherwise, GW checks the flag associated with the *TID*. If the flag is set then login is rejected due to multiple login attempts. If not then GW retrieves *vpw* from the database and computes A' and C_k'. GW verifies (C_k=C_k') to authenticate the SN and user. Otherwise, a reject message is sent to SN. GW computes V_s and V_u, time *t* is recorded in the database and the flag is set.

A2: GW sends the accept login message *(Acc_Login,* V_s, V_u , T_1*)* to the sensor node (SN).

A3: At time T_2, SN receives message from GW, computes V'_s and verifies (V_s=V'_s) to authenticate GW node and the user. SN then computes Y_u as shown in Figure 2.

A4: SN sends *(Acc_Login,* Y_u, T_2*)* to the UD.

A5: Upon receiving the message at time T_3, UD computes V'_u and Y'_u. If (Y_u=Y'_u) then SN and GW are authenticated and UD starts retrieving data from the SN. Otherwise, *Acc_Login* message is declined.

2.4 Password Change

Main steps of password change phase are as follows:

P1: UD chooses the new password PW_1 and computes vpw_1 that is the hash of PW_1.

P2: UD sends the triplet *(TID, vpw,* vpw_1*)* to GW via a secure channel.

P3: After verification of *TID* and *vpw*, GW generates nonce N_1 and computes TID_1, X_{1s} *and* TID'_1 as shown in Figure 2. GW updates *TID, vpw,* X_s and *TS.*

P4: GW sends success change, *Succ_Change (*N_1, X_s*)* to the UD.

P5: UD computes TID_1 and updates *TID* and X_s.

P6: The GW distributes (*TID,* TID'_1, X_{1s}, TS_1*)* to all the sensor nodes.

P7: Upon receiving updates, SN checks *TID* and computes TID_1. It also updates *TID,* X_s and *TS.*

3 SECURITY ANALYSIS

We assume that the adversary has the ability to replay, block or forge any network traffic. Moreover, it is computationally infeasible to break the cipher.

3.1 Performance Analysis

We have used computational overhead as a metric to compare the performance of our proposed scheme with the Vaidya et al.'s scheme (2009). The comparison of the computation is presented in Table 2. The number of elements contained in the messages is not considered for comparison. Our proposed scheme is slightly computationally expensive at GW. However, in most of the WSN applications, the computational capability of GW and user devices is higher than SN. The one-way Hash function and the XOR operation are considered lightweight for these two devices. It means that without adding any extra computational load for the SN, our authentication scheme provides higher security as compared to Vaidya et al.'s method (2009).

Table 2: Comparison of computational overhead.

Network Element	Authentication Scheme	
	Vaidya et al.'s Scheme	The Proposed Scheme
User (UD)	$5T_H + 1T_{XOR}$	$5T_H + 1T_{XOR}$
Gateway Node (GW)	$5T_H + 3T_{XOR} + (K+1)C_{MH}$	$6T_H + 3T_{XOR} + (K+1)C_{MH}$
Sensor Node (SN)	$3T_H + 2T_{XOR} + 1C_{MH}$	$3T_H + 2T_{XOR} + 1C_{MH}$
Total	$13T_H + 6T_{XOR} + (K+2)\ C_{MH}$	$14T_H + 6T_{XOR} + (K+2)\ C_{MH}$

The comparison of functional requirements can also be done easily. One can observe that the Vaidya et al.'s scheme (2009) does not resist multiple login and replay attack within a time interval. Their scheme uses timestamp to avoid replay attack. However, implementation of strict and safe time synchronization is difficult. In the case of a shorter transmission delay interval, a legal user's login can also fail. A large transmission delay will lead to replay attacks. On the other hand, our user authentication scheme provides better security features without adding any extra computation at SN. Our scheme inherently resists replay attack as it does not rely on network synchronization. The authentication latency time of our scheme is also low as it does not need to check the time interval.

3.2 Security Analysis

Our authentication scheme has all the security features of past schemes such as pseudo-nimity and resistance to password guessing, impersonation and replay attacks. It also incorporates mechanism to remove the flaws in Vaidya et al.'s schemes (2009; 2010).

Replay Attack of Login Message in the Login Step

L2: Our scheme can resist replay attack of login message. When an adversary eavesdrops the login message (*TID, A, t*) in the login step L2 and uses it to impersonate the *UD* to login the SN in a later session, our scheme resists this replay attack:

- The adversary replays the same previous message without modifying time, *t*. GW detects it as the time, *t* has already been recorded and the login will be denied by the GW.
- An adversary modifies the message and sends it to GW. ($C_k = C'_k$) will fail and GW denies the login.

Replay Attack of Accept Login Message in the Authentication Step A2 and A4: Our scheme can resist a replay attack on the accept-login message in the authentication step A2 in the following ways:

- While transmitting (Acc_Login, V_s, V_u, T_1) from GW to SN, the malicious party can intercept the message before forwarding it.
- In the next session when a legitimate SN sends (TID, C_k, T_0, t) to GW, the malicious party intercepts and drops that message to replay the captured *Acc_Login* message to SN pretending itself a legal GW.
- Since A' in V_s i.e. $H(X_s || A' || T_0 || T_1)$ is different from A in V'_s, the verification of ($V_s = V'_s$) will fail and the login will be rejected by SN.
- Alternatively, the malicious party can modify the *Acc_Login* message by replacing T_1 with T_{1e} and send the message to SN. Since T_1 in V_s is different from T_{1e} in V'_s, the verification of ($V_s = V'_s$) will fail and the login will be rejected by SN.

Similarly, the replay attack of accept login message in authentication step A4 is resisted by our method.

Replay Attack of Messages in Login Step L2 and Authentication Step A2: The adversary eavesdrops the login message in login step L2 and (*Acc_Login*, V_s, V_u, T_1) in the authentication phase step A2.

- The adversary replays the message *(TID, A, t)* to the sensor node. SN checks that the *TID* is a valid user and computes C_{ke} at time T_{0e}.
- The adversary blocks the message sent from the SN to GW in the login step L4 preventing the GW from receiving this message.
- The adversary replays (Acc_Login, V_s, V_u, T_1) message in the authentication step A2 to SN.
- SN receives message at T_{2e} and computes $V_s = H(X_s || A || T_0 || T_1)$ that is different from $V'_s = H(X_s || A' || T_{0e} || T_1)$ in the replayed message. In this way, login will be denied in the sensor node.

Forgery Attack with Node Capture Attack: Our user authentication scheme resists a forgery attack in two ways as given here.

After capturing SN, the adversary cannot compute C_k since A is not known or the verification of ($C_k = C'_k$) will fail and the login will be denied.

Gateway Bypass Attack Due to Node-capture Attack: If a user is allowed to access data from sensor node directly without GW node's notice then the impact of "node compromise" attack is very high. Our scheme resists gateway bypass attack.

- Adversary can compute $V_s' = H(X_s || A || T_{1e})$ in authentication step A3 but cannot compute V_u since vpw is not known. In this way, the gateway bypass attack is prevented in our scheme.

Many logged in user with same login ID threat: If a valid user shares its *TID* and password with another user, the other user can generate the login message and gain access to the login node. Our scheme can resist it as given below.

- GW records the time *t* against the *TID* and the flag of *TID* is changed from zero to one indicating that a user with this *TID* has logged in to the network. GW will decline such login requests.

Mutual Authentication: The proposed scheme can provide mutual authentication in the following way:

- UD_i is authenticated to GW by A = H(vpw||t)
- GW is authenticated to UD_i by V_u
- UD_i is authenticated to SN by *TID*
- SN is authenticated to UD_i by Y_u
- SN is authenticated to GW by C_k
- GW is authenticated to SN by V_s

4 PROTOCOL MODELING

We are evaluating the performance of our scheme under different attack scenarios. We have modelled a WSN using SystemC (2011). The SystemC based module architecture for our user authentication methodology is shown in Figure 3.

The WSN model consists of SystemC modules communicating through channels. Each module contains at least one process. Processes are activated according to a sensitivity list defined statically or dynamically. A module is made of communication and software models. The communication model emphasizes the communication between sensor, gateway, intruder and user modules. Software model consists of C++ processes representing sensor, gateway, user and other WSN components.

The user module generates the registration packet from the data provided by the user and sends the packet to gateway modules. The packet size used in our scheme is of 382 bytes length. The hash

function SHA-512 is used to generate the message digest in our scheme. However, 160 bit SHA-1 hash function can also be used to reduce the memory requirement for gateway (GW) and sensor modules.

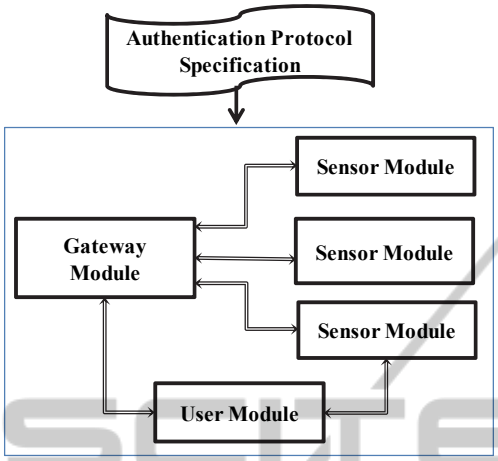

Figure 3: SystemC architecture of our protocol.

The authentication latency of our scheme is a function of the number of users, encryption cipher and channel transmission rate among the modules. We executed the simulation 20 times and observed that the average authentication latency of our scheme is 0.29 seconds (for one user). The effect of simultaneous multiple users' login requests on authentication latency is also being investigated. Replay, node capture, gateway bypass and multiple login attacks are further investigated by simulating our authentication protocol. It is verified that the protocol is resistant against all the above attacks that re-affirms our claims of Section 3. The main focus of our scheme is to provide application layer security. However, the security can further be enhanced by incorporating IEEE 802.15.4 (2003) specification at MAC sub-layer for all the phases of the proposed authentication protocol.

Finally, a memory requirement comparison is made between the Vaidya et al.'s scheme (2009) and our protocol. The user data storage requirements for both schemes are presented in Table 3. The storage requirement for sensor node in our scheme is slightly higher than Vaidya et al.'*s* scheme (2009). However, our protocol is resistant to replay as well as gateway bypass attacks.

Table 3: Comparison of storage overhead.

Storage Overhead per User (bits)			
	UD	*GW*	*SN*
Vaidya et al.'s scheme (2009)	2304	1600	1056
The Proposed scheme	2304	1601	1088

5 CONCLUSIONS

In this paper, we have proposed a robust user authentication scheme, which is an improved password-based authentication method. We have identified that Vaidya et al.'s scheme is subject to several security flaws (2009). To overcome these flaws, we have proposed an improved scheme that retains all the advantages of past user authentication schemes. Our proposed scheme resists replay, GW node bypass and many logged in user attacks. The scheme provides mutual authentication and resists replay attack inherently and does not require any network synchronization. We have modeled our protocol using SystemC and verified different attack scenarios. In our scheme, we have assumed that the database is securely stored in GW node and failing to meet this condition may make our scheme vulnerable to stolen verifier attack. Again none of the past schemes provides an inherent method to detect a compromised node.

REFERENCES

Benenson, Z., Gartner, F., & Kesdogan, D., (2004). User authentication in sensor networks, In *Proc. Workshop on Sensor Networks.* Informatik.

Benenson, Z., Gedicke N., & Raivio, O., (2005). Realizing robust user authentication in sensor networks, In Proc. *Workshop Real-World Wireless Sensor Networks,* Stockholm.

Das, M. L., (2009). Two-factor user authentication in wireless sensor networks, *IEEE Trans. Wireless Communication, 8,* 1086-1090.

IEEE Standard, 802.15.4-2003, (2003). *Wireless medium access control and physical layer specifications for low-rate wireless personal area networks*.

Khan, M. K., & Alghathbar, K., (2010). Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks, *Sensors*, *10*(3) 2450-2459.

Ko, L. C., (2008). A novel dynamic user authentication scheme for wireless sensor networks," In *Proc. IEEE ISWCS,* 608-612, Reykjavik Iceland.

Lee, T. H., (2008). Simple dynamic user authentication protocols for wireless sensor networks, *IEEE Sensor Communication, 43*, 657-660.

Sastry, N., & Wagner, D., (2004). Security considerations for IEEE 802.15.4 networks, In *Proc. ACM Workshop on Wireless Security*, 32-42.

SystemC. *The language for system-level modeling, design & verification*, IEEE Std. 1666-2011. Retrieved from http://www.accellera.org/downloads/standards/SystemC.

Tseng, H. R., Jan R. H., & Yang, W., (2007). An improved dynamic user authentication scheme for

wireless sensor networks, In *Proc. IEEE GlobeCom*. 986–990.

Vaidya, B., Makrakis, D., & Mouftah, H., (2010). Improved two-factor user authentication in wireless sensor networks, In *Proc. Int. Wks. Network Assurance & Security Services in Ubiq. Environments*, 600-605.

Vaidya, B., Rodrigues, J. J., & Park, J. H., (2009). User authentication schemes with pseudonymity for ubiquitous sensor network in NGN, *Int. Journal of Communication Systems, 23,* 1201-1222.

Wong, K. H., Zheng, Y, Cao, J., & Wang, S., (2006). A dynamic user authentication scheme for wireless sensor networks, In *Proc. IEEE SUTC, 1*, 318–327.

Zhou, X., Xiong, Y., Miao F., & Li, M., (2011). A new dynamic user authentication scheme using smart cards for wireless sensor network, In *Proc. IEEE Int. Conf. Computing, Control and Industrial Engineering,* 1-4.