

An Efficient Two-Factor User Authentication Framework for Wireless Sensor Networks

Pardeep Kumar¹, Mangal Sain¹ and Hoon Jae Lee²

¹Department of Ubiquitous-IT, Graduate School of Design & IT

²Division of Computer & Information Engineering
Dongseo University, Busan, 617-716, South Korea

Pardeepkumar@dit.dongseo.ac.kr, mangalsain1@gmail.com, hjlee@dongseo.ac.kr

Abstract- Nowadays, Wireless sensor networks (WSNs) are appeared to be new and promising solutions for next generation real-time wireless monitoring applications. These WSNs could become a threat if suitable security is not considered before the deployment. However, if there is any loophole in security, that might opens the door to attackers and hence, endanger for the applications. So, user authentication is one of the core requirements to protect WSNs data access from the unauthorized users. In this regard, we propose an efficient two-factor user authentication framework for WSNs, which is based on password and smart card (two-factors). Our scheme provides mutual authentication, enables the user to choose and change their password frequently. Moreover, the new framework provides strong protection against different kind of attacks at reasonable computation cost. In addition, we present analysis of our proposed framework security properties with the existing schemes in terms of overhead cost.

Keywords: Wireless sensor network security, user authentication, mutual authentication, password, smart card, two-factor.

I. INTRODUCTION

Recently, WSNs have been widely used in many real-time applications such as vehicular tracking, habitat monitoring, environment control, military surveillance, healthcare monitoring, wildlife monitoring, real-time traffic monitoring and so on. These wireless sensors facilitate ubiquitous nature, quick and easy deployment in any hostile environments to conveniently execute their tasks.

These sensor networks consist of discrete group of independent nodes with low cost, low power, limited computation, less memory and communicate wirelessly over limited frequency and low bandwidth [1]. Sensor nodes collectively monitor the area and sense substantial amount of data which is transmitted to the base-station using one node to another node via RF signals and routing schemes.

The potential development of WSNs applications has deal with many challenges such as security, architecture and protocol design issues. Therefore, state-of-art should pay attention, how to deploy sizeable WSNs.

Furthermore, providing security is very tedious task to these resource hungry sensor networks as compared to conventional networks such as local area networks (LANs) and wide area networks (WANs). While the WSNs security requirements are

the same as traditional networks, namely availability, confidentiality, integrity, authentication and non-repudiations. Thus, providing suitable security has emerged as one of the critical issue in wireless sensor networks.

In real-time WSNs, sensor data access queries are almost issued from the base-station nodes or backend application system. As the sensor nodes themselves provide services to users, it is necessary to control who is accessing the information and if it is authorized to do so. Thus, user authentication is possible solution to provide the access control from the unauthorized parties.

Although a numbers of significant authentication schemes have been proposed to provide adequate security at link layer [2 - 6] and network layer [7] for WSNs. However, WSNs user authentication at application layer is not been addressed effectively in order to prevent the access of sensor data from an unauthorized users. Furthermore, a review of current literature on WSNs reveals that only few user authentication schemes have been adequately addressed [8-16] at application layer.

In this paper, we present an efficient two-factor user authentication framework for WSNs, which impose on two-factor elements (e.g. password and smart card). The elements of two-factor authentication include “something you know” and “something you have” [17]. The first element (something you know), refer to a factor that is known by user such as a password. While, second element (something you have) refer to a something embedded on a device such as software token, digital certificate or biometric identifier (e.g. fingerprint scan and so on).

So, our proposed scheme attains the access control (user authentication) for wireless sensor networks, which resists to many attacks such as: user must have to login with same identity, replay attack, impersonation attack, stolen-verifier attack, password guessing attack, node-compromise attack, man-in-the-middle attack and denial-of-service attack. In addition, a user can change its password whenever demanded.

The rest of the paper is organized as follows: Section –II briefly reviews the related literatures with their weaknesses. In section –III we discuss the proposed two-factor user authentication scheme in details. Section-IV discusses the possible security analysis and performance evaluation as compared to existing schemes for WSNs and finally, section – V conclusions are drawn and future research directions.

II. LITERATURE REVIEW

In this section, we will discuss the literature reviewed for user authentication that has been recently proposed to verify the legitimacy of users for wireless sensor networks.

Benenson et al's [8] first sketched several security issues in WSNs, especially the access control and proposed the notion of n -authentication, where user can successfully authenticate with at least $(n-t)$ of n -sensors, where t is the number of sensor nodes that the adversary can compromise. Subsequently, Benenson et al's [9] proposed another solution for user authentication problem in the presence of node capture attacks. The proposed scheme is based on *public key cryptography (PKC)* and *elliptic curve cryptography (ECC)*. Some major weaknesses were pointed out on Benenson et al. scheme, such as impersonation attack, denial-of-service (DoS) attacks could be mounted by sending many bogus signatures in authentication phase [10]. Moreover, the computation cost of PKC and ECC is very high for sensor networks.

Wong et al's [10] proposed a dynamic user authentication scheme for wireless sensor networks, which is based on password. This scheme imposes on very light computation cost that requires only one-way hash function and simple *XOR* operations. The scheme consists of three phases: registration phase, login and authentication phase. Unfortunately, Wong et al scheme is vulnerable to many attacks such as replay attacks, forgery attacks, stolen-verifier attacks and password guessing attacks [11-12, 14 and 18].

Tseng et al's [11] enhanced the weaknesses of Wong et al's scheme and proposed an improved dynamic user authentication scheme for wireless sensor networks. The proposed scheme retains all the advantages of Wong et al's scheme and improved security features with better efficiency such as: resistance to replay, forgery attacks and reduction of user password leakage risk. In addition, it allows users to change their password freely whenever demanded.

T. H. Lee [12] proposed a simple dynamic user authentication scheme for WSNs, which is the variant of strong password-based solution. T. H. Lee scheme is more simplified in term of authentication process by reducing the computational load, communication cost and furthermore, an intruder cannot impersonate the gateway node.

L. C. Ko [13] pointed out some weaknesses of Tseng et al's scheme that might cause user authentication mechanism insecure. Since, Tseng et al's scheme achieves many enhanced measure upon Wong et al's scheme. In addition, Tseng et al's does not achieve mutual authentication between the gateway and the sensor nodes and between the user itself and the sensor nodes. L. C. Ko proposed a novel dynamic user authentication scheme for WSNs, which provides better security features than Tseng et al's scheme.

Watro et al's [4] proposed a public key based scheme called TinyPK, which allows authentication and RSA-based Diffie-Hellman key agreement between sensor network and third party as well as between two sensor networks. To reduce the computational complexity, a small public exponent (e.g. $e=3$) is used, which is very small variant of RSA. Furthermore,

TinyPK protocol is vulnerable to "masquerade as sensor node to an unknowing user attack [18]".

Banerjee and Mukhopadhyay [15] proposed a symmetric key based authenticated querying in wireless sensor networks, which imposed on random polynomial key pre-distribution scheme. This scheme authenticates the user agent but vulnerable to "user agent capture attack," (e.g., when a user agent is compromised, an attacker can get all the information from any sensor node).

Yoon et al's [16] proposed a user authentication scheme with privacy protection for WSNs, which is the variant of Kerberos protocol. The key idea behind this scheme is, it provides mutual authentication between trusted third party and both user agent and sensor node. Beside, Yoon et al's scheme also provides the privacy protection to the user.

Recently, M. L. Das [18] mentioned some security flaw in Wong et al's schemes, such as, the scheme vulnerable to many logged in user with the same login-id threat and also susceptible to stolen-verifier attacks. M. L. Das proposed a two-factor user authentication for WSNs, where the legitimate users must prove the possession of both a password and smart card. Das's claimed that his scheme is secure against many attacks (e.g. user authentication, replay, guessing, impersonation, node compromise, stolen-verifier, DoS attacks).

Nyang and Lee [19] identified that Das's scheme is still vulnerable to an offline password guessing attack by insider, node compromise attack and does not care about other security services, i.e., encryption and authenticity verification of query response. Hence, Nyang and Lee proposed an enhanced two-factor user authentication protocol for WSNs, which overcome the Das's scheme security flaws with some additional security services such as, confidentiality and authenticity of user's query response.

More recently, Khan and Alghathbar [20] pointed out that M.L. Das scheme is still not secure and cannot resist to many other security attacks, such as, gateway-node bypass attack, does not provides mutual authentication between gateway and sensor nodes, vulnerable to insider attack, and no provision for users to change their password. Khan and Alghathbar overcomes the security weaknesses of Das's scheme and proposed improved two-factor user authentication in WSNs, which provides protection against insider attack, gateway bypass attack and introduced password change phase for users.

III. PROPOSED FRAMEWORK

In this section, we propose a user authentication framework for wireless sensor networks that ensures the access and supply of data are taking place by the legitimate users only. So, in this regards, a user must register with the gateway node in a secure manner to access the real time sensors data. Upon the successful user registration, the gateway node personalizes a smart card to every registered user. Then, a user can submit his/her query in an authentic way and access the sensor networks data at any time within an administrative configurable period [10]. The framework is divided into four

phases, namely, user registration phase, login phase, authentication phase and password change phase. For convenience Table 1, a list of some notations and symbols will be used throughout the rest of paper.

TABLE 1
NOTATION AND SYMBOL USED IN PAPER

Notation	Descriptions
U_k	User k^{th} to be login
ID_k	Login_ID of U_k
PW_k	Password of U_k
FID_k	fictitious ID of U_k
$GW\ node$	WSN gateway node
Sn	Sensor Node
X_g	Secret parameter generated by $GW\ node$
$h(.)$	Cryptographic hash function
$\oplus$	Bitwise XOR function
$\parallel$	Bitwise concatenation function

We have made the following assumptions for two-factor user authentication framework:

- All the nodes locations are static.
- The $GW\ node$ is considered as trusted node.
- Each user who wishes to access the sensor network data, he/she must register once with the $GW\ node$.
- The secret parameter X_g is not known to the user, since; it is generated and securely stored in user's smart card by the $GW\ node$.

(A). Registration Phase (RP)

In the registration phase, initially, each user must register him/her with the $GW\ node$ using following steps:

RP-1). The user U_k submits his/her identity and password (i.e., ID_k and PW_k) to the $GW\ node$ over a secure channel.

RP-2). Upon receiving the U_k registration request, the $GW\ node$ computes:

- $h(PW_k)$
- $h(X_g)$
- $N_k = h(ID_k \parallel h(PW_k) \parallel h(X_g))$

Thereafter, the $GW\ node$ personalizes a smart card to the user with the parameters $\{h(.), ID_k, N_k, h(PW_k), h(X_g)\}$, here, X_g is secret parameter securely generated and hashed by the $GW\ node$. Furthermore, $h(X_g)$ is stored in the sensor nodes prior to deployment of the sensor nodes, who wish to exchange their data with the users. This step completes the user's registration phase.

(B). Login Phase (LP)

This phase invoked whenever a user U_k wants to submit his/her query to access the sensor networks, then every time he/she has to accomplish the login phase. The user U_k inputs

his ID_k and PW_k and inserts his smart card in the terminal. Now, smart card confirms the entered ID_k and PW_k with the pre-stored values (ID_k and PW_k). If the entered ID_k and PW_k are not verified then reject the login request. Otherwise, smart card executes some functions and performs following:

LP-1). Compute $FID_k = h(ID_k \parallel h(PW_k) \parallel h(X_g)) \oplus h(h(X_g) \parallel T)$, here, T is denoting the current timestamp of U_k 's system.

LP-2). Compute $C_k = h(N_k \parallel h(X_g) \parallel T)$

LP-3). Now, this is end of the login phase and user login request message $\langle FID_k, C_k, T \rangle$ is send to the $GW\ node$ over a secure channel for the authentication process.

(C) Authentication Phase (AP)

The authentication phase is invoked when it receives the user's login request message $\langle FID_k, C_k, T \rangle$ at time T' . Now, the $GW\ node$ authenticates user requests by the following steps:

AP-1). The $GW\ node$ validate the T : check, if $(T' - T) \geq \Delta T$, if yes, then the $GW\ node$ rejects this request and terminate the process. Otherwise, continues with next step. Here, T' is the current timestamp of the $GW\ node$ and ΔT is the expected time interval for the transmission delay.

AP-2). Computes

: $h(ID_k \parallel h(PW_k) \parallel h(X_g)) = FID_k \oplus h(h(X_g) \parallel T)$,
and $C_k = h(h(ID_k \parallel h(PW_k) \parallel h(X_g)) \parallel h(X_g) \parallel T)$.

AP-3). Thereafter check: if $(C_k^* = C_k)$ holds then the $GW\ node$ accepts the login request, and proceeds to next step, otherwise request rejects and terminates the further operations.

AP-4). And the $GW\ node$ computes:

$A_k = h(FID_k \parallel Sn \parallel h(X_g) \parallel T'')$.

AP-5). Now, the $GW\ node$ sends a user's request message $\langle FID_k, A_k, T'' \rangle$ over a communication channel to some nearest sensor node (e.g., Sn), which user was demanding. Here, message $A_k = h(FID_k \parallel Sn \parallel h(X_g) \parallel T'')$ and T'' is the current timestamps of the $GW\ node$. Furthermore, A_k make sure to the sensor node that the request message $\langle FID_k, A_k, T'' \rangle$ has comes from the authentic $GW\ node$ and not from the fake. Since, A_k is computed with help of the $GW\ node$ secret parameter ($h(X_g)$), which is known to the $GW\ node$ and securely stored in the sensor nodes.

AP-6). Now, Sn validate the time T'' : check, if $(T''' - T'') \geq \Delta T$, if yes, then the sensor node (Sn) rejects the request and terminate the process, otherwise continues with next step. Here, T''' is the current timestamp of the sensor node and ΔT is the expected time interval for the transmission delay.

AP-7). Sn now computes $A_k^* = h(FID_k \parallel Sn \parallel h(X_g) \parallel T''')$ and check: if $(A_k^* = A_k)$ holds then the sensor node respond to user's requested query. Otherwise rejects the request and terminates the further operations.

AP-8). Sn now computes message $M_k = h(Sn \parallel h(X_g) \parallel T''''')$ and provide mutual authentication to the $GW\ node$. Here, T''''' is the current timestamp of Sn node's and sends message $\langle M_k, T''''' \rangle$ to the $GW\ node$.

AP-9). Upon receiving the message $\langle M_k, T''''' \rangle$, the $GW\ node$ validate the time T''''' : check, if $(T^* - T''''') \geq \Delta T$, if yes, then the $GW\ node$ rejects the request and terminate the process,

otherwise continues with next step. Here, T^* is the current timestamp of *GW node* and ΔT is the expected time interval for the transmission delay.

AP-10) The *GW node* now computes $M_k^* = h(Sn || h(X_g) || T''')$ and check: if $(M_k^* == M_k)$ holds then mutual authentication is take places between the sensor node *Sn* and the *GW node*. Otherwise, *Sn* is not an authentic node and the *GW node* terminates the operations.

AP-11). Upon the successful mutual authentication between the sensor node *Sn* and the *GW node*, user U_k starts the access of sensor data.

(D) Password-Change Phase (PP)

The password change phase is invoked whenever user U_k wants to change or update his/her old password (PW_k) to a new password, say PW_k^* . The password change phase is described in the following:

PP-1). User U_k inserts his/her smart card into the terminal and enters his/her identity (ID_k) and password (PW_k).

PP-2). Now the smart card validates the U_k 's entered ID_k and PW_k with stored values and check: if holds then the smart card request to the user for new password (i.e., PW_k^*). Otherwise, rejects the password change request and terminates the operation.

PP-3). Now upon receiving the U_k new password (PW_k^*), smart card computes: $N_k^* = N_k \oplus h(ID_k || h(PW_k) || h(X_g)) \oplus h(ID_k || h(PW_k^*) || h(X_g))$, here N_k is old stored value of the smart card (i.e., $N_k = h(ID_k || h(PW_k) || h(X_g))$).

PP-4). Now the smart card replaces the old values (N_k and $h(PW_k)$) with new values (N_k^* and $h(PW_k^*)$).

After performing the above steps, password change phase successfully takes places.

IV. ANALYSIS OF FRAMEWORK

In this section, we present our proposed two-factor framework strength in terms of security analysis (i.e., resist against several well-known attacks) and performance analysis.

(A) Security Analysis

Now we will shows the proposed framework that resists against the following attacks: such as, replay attack, impersonation attack, stolen-verifier attack, password guessing attack, node-compromise attack, man-in-the-middle attack, denial-of-service attack. Furthermore, our framework consider mutual authentication between the *GW node* and the sensor node and enable users to change their password freely whenever required.

Replay attack. Our two-factor framework is secure against a replay attack, because the authenticity of messages $\langle FID_k, C_k, T \rangle$, $\langle FID_k, A_k, T'' \rangle$ and $\langle M_k, T''' \rangle$ is validated by checking the freshness of three timestamps $(T'-T) \geq \Delta T, (T'''-T'') \geq \Delta T$ and

$(T^*-T''') \geq \Delta T$. Thus, our framework is secure against replaying of message.

Impersonation attack. An attacker cannot impersonate the user, suppose, an attacker captures a login message $\langle FID_k, C_k, T \rangle$. Now, he/she will wish to login again into the system, but this is not feasible to get the original password (PW_k) and secret (X_g), since, they are hashed with the cryptographic hash functions. Therefore, it is not possible to impersonate the user.

Stolen-verifier attack. Stolen-verifier attack is not applicable to our framework, because we are not using any password/verifier table. So, any kind of stolen verifier attack will not occur on our framework.

Password guessing attack. Since, our framework is free from any password verifier table, so password guessing attack is not feasible. Furthermore, in login phase the password is not simply transmitted but it is transmitted with some other secrets, which is difficult to guess the user password.

Node-compromise attack. In general, sensors are placed in the hostile environment to do their task. Therefore, it could easy to capture a node from the environment and steals stored secret information about the networks. In order to overcome this attack, we store hashed secret values in sensor node, as, $A_k = h(FID_k || Sn || h(X_g) || T'')$. Thus, by doing so, it is difficult to get the secret parameters in the case of node compromised.

Man-in-the-middle attack. An attacker may attempt a man-in-the-middle (MITM) by modifying the login message $\langle FID_k, C_k, T \rangle$ into $\langle FID_k^*, C_k^*, T^* \rangle$. However, this malicious attempt will not works, because without the knowledge of X_g , it is not easy to calculate the message $\langle FID_k^*, C_k^*, T^* \rangle$. Thus, man-in-the-middle attack is not applicable in our framework.

Denial-of-service attack. In password change phase, denial-of-service attack cannot work in our framework. Suppose, when user smart card is stolen, unauthorized users cannot change new password. Since, in password change phase the old ID_k and PW_k is verified first. Hence, denial-of-service attack is not applicable on stolen smart.

Secure password change. In secure password change or update phase, our framework first verifies the old password, identity and then only request for new password. Otherwise rejects the password change requests. Therefore, our framework change password securely.

(B) Performance Analysis

Here we examine the performance and summarize the security functionality of our two-factor framework and compare with the M.L. Das [18] two-factor scheme. Table –II shows that our framework is more secure and robust as compares to Das's scheme and provides more security features on reasonable computational costs.

As shown in Table-II, our two-factor framework has 13H computational cost and provides robust security features, such as, secure password change phase, provide mutual authentication, secure against node compromised attack and secure against denial-of-service attack and secure against many other attacks.

TABLE-II
PERFORMANCE ANALYSIS

Security Features	Our Scheme	Das's[18]
Secure password change phase	Yes	No
Provides mutual authentication	Yes	No
Secure against node compromised attack	Yes	No
Secure against denial-of-service	Yes	No
Registration phase computational cost	3H	2H
Login phase computational cost	3H	3H
Authentication/verification phase cost	7H	5H

H: a cryptographic hash function

V. CONCLUSION

In this paper, we have proposed an efficient user authentication framework for wireless sensor networks, which is imposed on two-factors (i.e., password and smart card) and using cryptographic hash functions. We have provided security and performance analysis of the proposed framework and compared with M.L. Das scheme. Furthermore, we have demonstrated that our proposed framework is more robust against many security attacks and provides essential security features on the reasonable computational costs.

An interesting user authentication research is currently under investigation and we will enhance the proposed framework with more security features.

ACKNOWLEDGMENT

This research is supported by 2010 National Research Foundation (NRF) project, South Korea.

REFERENCES

- [1] I.F. Akyildiz, W. Su, Y. Sankarasubramamiam and E. Cayirci, "A Survey on Sensor Network," IEEE Communication Magazine, August 2002, pp. 102-114.
- [2] A. Perrig, R. Szewczyk, V. Web, D. Culler and J.D. Tygar, "SPINS: Security Protocol for Sensor Networks," Proceeding of 7th Annual International Conf on Mobile Computing and Networks (MOBICOM 2001), Rome, Italy. July 2001.
- [3] C. Karloff, N. Sastry and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks," Proc. of 2nd ACM Conf. on Embedded Networked Sensor System (SenSys 2004), Baltimore, MD, November 2004.
- [4] R. Watro, D. Kong, S-F Cuti, C. Gardiner, C. Lynn and P. Kruus, "TinyPK: Securing Sensor Networks with Public Key Technology," Workshop on Security of Ad-hoc and Sensor Networks, Washington DC, USA 2004.
- [5] M. Luk, G. Mezzour, A. Perrig and V. Gligor, "MiniSec: A Secure Sensor Network Communication Architecture," IPSN'07, April 2007, Cambridge, Massachusetts, USA.
- [6] P. Kumar, S. Cho, D-S Lee, Y-D Lee and H-J Lee, "TriSec: A Secure Data Framework for Wireless Sensor Networks Using Authenticated Encryption," International Journal of Maritime Information and Communication Sciences, April 2010, vol 8 no. 2, pp.129-135.
- [7] C. Karlof, and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasure," in proc of 1st IEEE International Workshop on Sensor Network Protocols and Application.
- [8] Z. Benenson, F. Gartner, and D. Kesdogan, "User Authentication in sensor network (extended abstract)," In proceeding of informatics 2004, Workshop on Sensor networks, September 2004.
- [9] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authentication in sensor networks," Workshop on Real-World Wireless Sensor Network (REALWSN'05).
- [10] K. H. M. Wong, Y. Zheng, J. Cao, S. Wang, "A Dynamic User Authentication Scheme for Wireless Sensor Networks," In the proceeding of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), 2006.
- [11] H. R. Tseng, R. H. Jan, and W. Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks," IEEE GLOBECOM 2007, pp. 986-990.
- [12] T. H. Lee, "Simple Dynamic User Authentication Protocols for Wireless Sensor Networks," 2nd International Conference on Sensor Technologies and Application (SENSORCOMM'08), pp. 657- 660.2008.
- [13] Lee-Chun Ko, "A Novel Dynamic User Authentication Scheme for Wireless Sensor Networks," In the Proceeding of IEEE ISWCS 2008, pp. 608-612.
- [14] B. Vaidya, J. J. P.C. Rodrigues, and J. H. Park, "User Authentication Schemes with pseudonymity for Ubiquitous Sensor Network in NGN," International Journal of Communication Systems, 2009.
- [15] S. Banerjee and D. Mukhopadhyay, "Symmetric Key Based Authenticated Querying in Wireless Sensor Networks," In Proceeding of 1st ACM International Conference on Integrated Internet Ad hoc and Sensor Networks (InterSense), 2006.
- [16] S. J. Yoon, H. Lee, S. B. Ji, and K. Kim, "A User Authentication Scheme with Privacy Protection for Wireless Sensor Networks,"
- [17] <http://www.rsa.com/node.aspx?id=1156>
- [18] M. L. Das, "Two-Factor User Authentication in Wireless Sensor Networks," IEEE Transaction on Wireless Communication, Vol.8, No.3, March 2009, pp. 1086-1090.
- [19] D. H. Nyang and M. K. Lee, "Improvement of Das's Two-Factor Authentication Protocol in Wireless Sensor Networks," <http://eprint.iacr.org/2009/631.pdf>.
- [20] M. K. Khan and K. Alghathbar, "Cryptanalysis and Security Improvement of 'Two-Factor User Authentication in Wireless Sensor Networks'," Sensors 2010, pp. 2450-2459.