Robust Dynamic User Authentication Scheme for Wireless Sensor Networks

Binod Vaidya
Instituto de Telecomunicações
Rua Marquês D'Ávila e Bolama
6201-001Covilhã,
PORTUGAL
bnvaidya@co.it.pt

Jorge Sá Silva
Dep. Informatics Engineering,
University of Coimbra
Polo II - Pinhal de Marrocos,
3030-290 Coimbra
PORTUGAL
sasilva@dei.uc.pt

Joel J. P. C. Rodrigues
Instituto de Telecomunicações
University of Beira Interior
Rua Marquês D'Ávila e Bolama
6201-001Covilhã
PORTUGAL
joel@ubi.pt

ABSTRACT
In recent years, wireless sensor networks (WSNs) have been widely used in different domains. For instance, WSNs can be deployed in insecure and unattended environments. In this regard, user authentication is a critical issue for WSNs. In this paper, we propose a user authentication protocol in WSNs, which is variation of strong-password based solution proposed by Wong *et al.* The proposed protocol is evaluated and compared with the previous schemes.

Categories and Subject Descriptors
C.2.0 [Computer-Communication Networks]: General - Security and protection; C.2.1 [Computer-Communication Networks]: Network Architecture and Design - Wireless communication; K.6.5 [Management of Computing and Information Systems]: Security and Protection - Authentication

General Terms
Algorithms, Design, Security

Keywords
Wireless sensor network, strong-password based authentication, user authentication.

1. INTRODUCTION
Wireless sensor networks (WSNs) consist of many sensor nodes that are deployed on areas where collecting data from it. Sensor networks can be used in a wide variety of applications, for instance, structural health monitoring, environmental control, vehicular tracking, military operations or surveillance.

The sensors are cheap, small devices with battery and memory constraints and little computation power. However, when the number of sensors in the network is large or the deployment area is inaccessible, replacing node is very costly or impossible.

In many applications, the real-time data may no longer be accessed at the gateway node only. It can be accessed from any sensor login node in an ad hoc manner. Providing user authentication to access real-time data is critical. Hence, to prevent unauthorized users from gaining the information, robust user authentication scheme is required.

Several user authentication schemes [1-7] have been proposed to prevent from unauthorized users from gaining access to the system. However, only few schemes [1-4] have been proposed those are well suited for WSNs.

Wong *et al.* [2] proposed a lightweight strong-password based dynamic user authentication protocol for WSNs. Wong *et al*. scheme uses basically one-way hash function and exclusive-OR operation to provide the dynamic user authentication in WSN. It consists of three phases: Registration, Login, and Authentication.

Tseng *et al*. [4] proposed an improved user authentication scheme that is modification of Wong *et al*.'s scheme such that it not only fixes the weaknesses but also enhances the security of Wong *et al*.'s scheme. Tseng *et al.*'s scheme is divided into four phases: registration, login, authentication, and password-changing phases.

However, both the schemes still have security flaws and cannot fully prevent from various malicious attacks. In this paper, we propose robust dynamic user authentication scheme for WSN, which is a variation of strong-password based solution proposed by Wong *et al.* [2]. Our scheme can provide better security features than two above-mentioned schemes.

2. CRYPTANALYSIS
In this section, we show some of the security weaknesses for Wong *et al*.'s scheme [2], and Tseng *et al.*'s scheme [4].

Wong *et al*'s scheme is vulnerable to several attacks such as forgery attack, and replay attack.

Forgery attack can be occurred in following manner. Adversary captures LN to obtain *UID, A, TS* and eavesdrops *UID, PW*. Then it computes $B_e = H(A \,||\, H(PW))$; $C_{1e} = H(T' \oplus B_e)$; $C_{2e} = B_e \oplus A$. It sends message (UID, C_{1e}, C_{2e}, T') to GW. As long as $(T - T') < \Delta T$ then it is passed.

Replay attack of *Acc_login* can occur as follows. While transmitting *Acc_login* from GW to LN, the malicious

Q2SWinet'09, October 28–29, 2009, Tenerife, Canary Islands, Spain.

intermediate node can intercept it before forwarding it. In next session when this adversary receives message to GW from legitimate LN, it just drops that message and the captured *Acc_login* is replayed to LN as pretending legal GW.

Tseng *et al*'s scheme cannot thwart some attacks such as replay attack, and man-in-the-middle (MITM) attack.

Replay attacks of *Acc_login* can be possible as follows. While transmitting *Acc_login* from GW to LN, the malicious intermediate node can intercept it before forwarding it. Next time when this malicious node receives message to GW from legitimate LN, it just drops that message and the captured *Acc_login* is replayed to LN as pretending legal GW. LN does not check the correctness, so it will also send *Acc_login* to UD.

In case of MITM attack, *UID, A, t* is intercepted or eavesdropped by an adversary. It then intercepts *UID, C, T, t*. After computing $C^* = H(A \oplus T^*)$, it will forward *UID, C*, T*, t* to GW.

3. PROPOSED AUTHENTICATION PROTOCOL

In this section, we propose a user authentication scheme to overcome above-stated weaknesses and improve security.

Table 1. Notations used

Symbols	Descriptions
UD	User's Device such PDA, PC
GW	Registration Sensor Gateway
LN	Sensor Login node
$H( )$	One-way hash function
N_0 , N_1	Random nonces
$\oplus$	Exclusive-or (XOR) operation
$\|\|$	Concentration
Succ_Reg	Successful Registration message
Acc_login	Accept login message
Succ_Change	Successful Changes message
x	Secret key known to the GW
UID	User's identity
PW	Password chosen by user
TS	Timestamp for particular user
t, T, T_0	Current time recorded by one of the nodes
ΔT	Allowed time interval for transmission delay

Table 1 shows the notations used in the proposed scheme. In the proposed scheme, it is assumed that as one-hop communication between UD and LN occurs, it is less likely to have malicious action. So we have only considered mutual authentication between GW and LN. The proposed scheme is composed of four phases: registration phase, login phase, authentication phase, and ID/password change phase.

In Registration phase, the UD randomly chooses a password *PW* and calculates $vpw = H(PW)$. Afterwards, the UD submits its identity *UID* and *vpw* to the GW in a secure way. The GW computes $X = H(UID \,||\, x)$. Then the GW replies to the user for successful registration, stores (*UID, vpw, X, TS*), and distributes *(UID, X, TS)* to those sensor nodes, which are able to provide a login interface to users.

RP1 -	UD	:	Compute $vpw = H(PW)$
RP2 -	UD → GW	:	*UID, vpw*
RP3 -	GW	:	Compute $X = H(UID \,||\, x)$
			Store *UID, vpw, X, TS*
RP4 -	GW → UD	:	*Succ_Reg*
RP5 -	GW → LNs	:	*UID, X, TS*
RP6 -	LN	:	Store *UID, X, TS*

In Login phase, a user submits (*UID, A, t)* to a login node. Upon receiving the login request at time T_0 , the login node checks its lookup table to see if *UID* is a valid user and checks $T_0 - t \geq \Delta T$. The login request is rejected if it is not. Otherwise, the login node retrieves the corresponding *A* and computes $C_K = (X \oplus A \oplus T_0)$. It then sends ($UID, C_K, T_0, t$) to the GW.

LP1 -	UD	:	Compute $A = H(vpw \,||\, t)$
LP2 -	UD → LN	:	*UID, A, t*
LP3 -	LN	:	Check *UID*
			Check $T_0 - t \geq \Delta T$
			Compute $C_K = (X \oplus A \oplus T_0)$
LP4 -	LN → GW	:	UID, C_K, T_0, t

In Authentication phase, the GW checks whether or not *UID, t* is a valid user and *t*. The login request is rejected if it is not. Otherwise, the GW verifies if $T_1 - T_0 \geq \Delta T$; $T_0 - t \geq \Delta T$. If the condition is satisfied, then the login request is considered as a replay message and thus is rejected. On the other hand, the GW retrieves the corresponding *vpw* and A and computes $A' = H(vpw \,||\, t)$ and $C_K' = (X \oplus A' \oplus T_0)$. A reject message is sent to the login node if $C_K \neq C_K'$. Otherwise, computes $V_M = H(X \,||\, A' \,||\, T_1)$ and sends accept message (Acc_login, V_M, T_1) is sent to the login node which is forwarded to the user.

AP1 -	GW	:	Check *UID, t*
			Check $T_1 - T_0 \geq \Delta T$; $T_0 - t \geq \Delta T$
			Compute $A' = H(vpw \,||\, t)$
			Compute $C_K' = (X \oplus A' \oplus T_0)$
			Verify $C_K = C_K'$
			Compute $V_M = H(X \,||\, A' \,||\, T_1)$
			Store *t*
AP2 -	GW → LN	:	Acc_login, V_M, T_1
AP3 -	LN	:	Check $T_2 - T_1 \geq \Delta T$
			Compute $V'_M = H(X \,||\, A \,||\, T_1)$
			Verify $V_M = V'_M$
AP4 -	LN → UD	:	*Acc_login*

In the Password-changing phase, UD changes his password *PW* to PW_1. Then it computes $vpw_1 = H(PW_1)$ and sends the triple (UID, vpw, vpw_1) to the GW in the secure channel. The GW computes X_1 and sends success change *Succ_Change* to the UD. At the same time, the GW distributes updated information to all the LNs. Upon receiving updates, LNs obtain TID'_1 and update their databases.

PP1 - UD : Compute $vpw_1 = H(PW_1)$
PP2 - UD → GW : *UID, vpw, vpw_1*
PP3 - GW : Compute $X_1 = H(UID_1 || x)$
Updates *UID, vpw, X, TS*
PP4 - GW → UD : *Succ_Change*
PP5 - GW → LNs : *UID, X_1, TS_1*
PP6 - LN : Updates *UID, X, TS*

The partial communication flows of the proposed scheme are shown in Figure 1, in which registration, login and authentication phases are shown, whereas Figure 2 shows communication flow for password-changing phase.

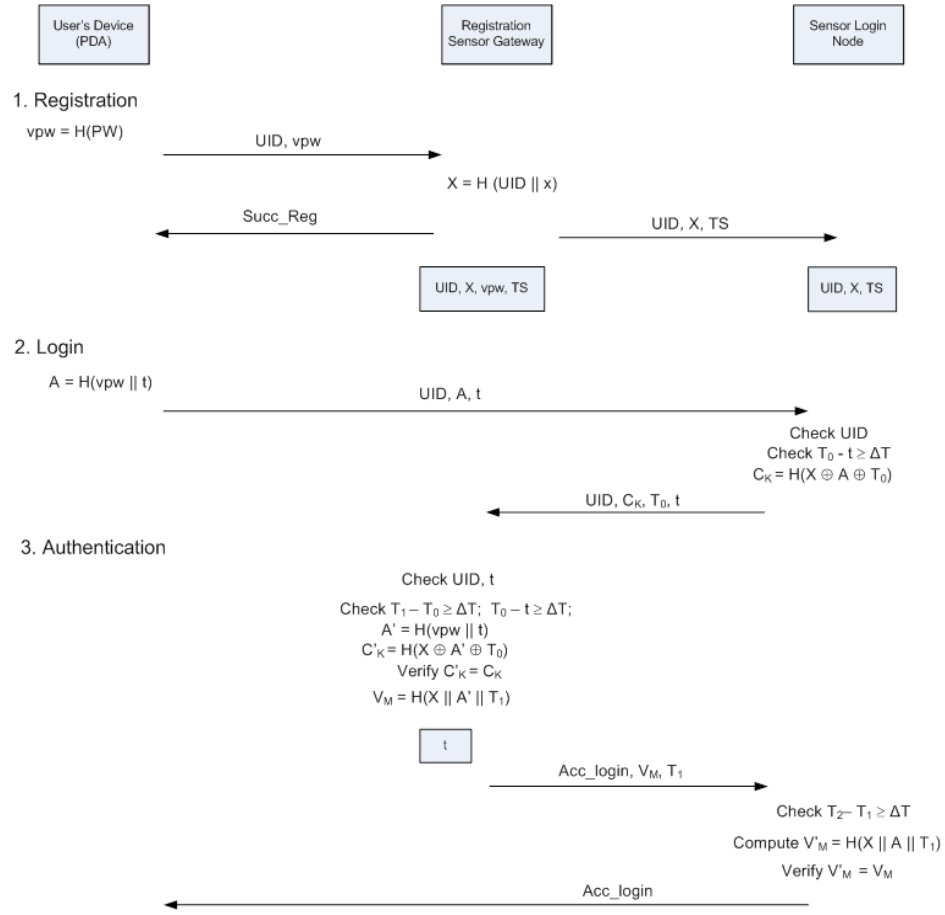

Figure 1. Partial Communication flows for proposed scheme.

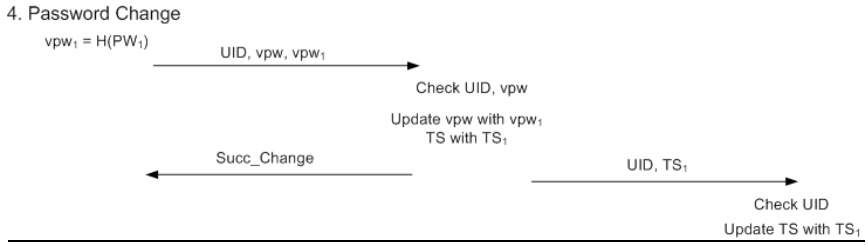

Figure 2. Password changing phase for proposed scheme.

4. ANALYSIS

In this section, we present the security analysis of the proposed scheme and the comparison of the cost overhead with some existing schemes.

4.1 Security Analysis

The proposed scheme has several advantages over the existing schemes. It has following security features.

The proposed scheme can provide protection against the replay attacks of login message as well as accept login message (*Acc_login*). In case of login message, as GW-node checks user ID and timestamp, the adversary node cannot replay it, whereas in case of *Acc_login* message, as a login node checks the authenticator, the adversary node cannot replay it.

The proposed scheme can protect against the forgery attacks. In both schemes, the adversary node could not be able to compute C_k as it has no knowledge of the value of A. And if the adversary tries forgery attack using login message, it still cannot have access because of the timestamp used.

The proposed scheme can protect against the MITM attacks. In both schemes, the adversary node could not be able to compute C_k as it has no knowledge of the value of X.

The proposed scheme provide mutual authentication between login node and gateway node. A gateway node verifies the authenticator containing C_k supplied by the login node while a login node verifies the authenticator containing X furnished by a gateway node.

4.2 Overhead Cost Comparisons

Table 2 summarizes the comparisons of the Wong *et al*.'s scheme, Tseng *et al*.'s scheme and proposed scheme in terms of cost overheads.

Table 2. Overhead Cost Comparison

Protocols	Overhead Cost			
	Registration	Login	Authentication	Total
Wong *et al*.'s scheme [2]	$3T_H+1C_{MH}$	$3T_H+2T_{XOR}+1C_{MH}$	$1T_H+2T_{XOR}+1C_{MH}$	$7T_H+4T_{XOR}+3C_{MH}$
Tseng *et al*.'s scheme [4]	$1T_H+1C_{MH}$	$2T_H+2T_{XOR}+1C_{MH}$	$2T_H+2T_{XOR}+1C_{MH}$	$5T_H+4T_{XOR}+3C_{MH}$
Proposed scheme	$2T_H+1C_{MH}$	$2T_H+2T_{XOR}+1C_{MH}$	$4T_H+2T_{XOR}+1C_{MH}$	$8T_H+4T_{XOR}+3C_{MH}$

In Table 2, T_H, T_{XOR}, and C_{MH} represent, respectively, time for performing a one-way hash function, time for performing an XOR operation, and the delay time for the communication taken place between login node and GW-node in multi-hops. The number of elements contained in transmitted messages is not considered in the comparison.

It can seen that the computational cost of the proposed scheme is almost similar to Wong *et al.*'s scheme and slightly higher than Tseng *et al*'s scheme in terms of the first three phases (registration, login, and authentication). However, the proposed scheme has advantage over both the existing schemes as the former has better security features.

5. ACKNOWLEDGMENTS

Part of this work has been supported by *Instituto de Telecomunicações,* Next Generation Networks and Applications Group (NetGNA), Portugal, and by the Euro-NF Network of Excellence of the Seventh Framework Programme of EU.

6. REFERENCES

[1] Benenson, Z., Gedicke, N., and Raivio, O. 2005. Realizing Robust User Authentication in Sensor Networks. In Proceedings of Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), Sweden, June 2005.

[2] Wong, K. H. M., Zheng, Y., Cao J., and Wang, S. 2006. A dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06) Jun. 2006; 1: 318–327.

[3] Jiang, C., Li, B., and Xu, H. 2007. An Efficient Scheme for User Authentication in Wireless Sensor Networks. In Proceedings of 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007.

[4] Tseng, H. R., Jan, R. H., and Yang, W. 2007. An improved dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE Global Communications Conference (GLOBECOM'07), Nov. 2007; 986-990.

[5] Das, M. L., Saxena, A., and Gulati, V. P. 2004. A Dynamic ID-based Remote User Authentication Scheme. IEEE Transactions on Consumer Electronics, May 2004; 50(2):629–631.

[6] Yoon, E. J., Ryu, E. K., and Yoo, K. Y. 2005. An improvement of Hwang Lee Tang's simple remote user authentication scheme. Elsevier Computers & Security, Feb. 2005; 24(1):50–56.

[7] Wang, Y. Y., Liu, J. Y., Xiao, F. X., and Dan, J. 2009. A more efficient and secure dynamic ID-based remote user authentication scheme. Elsevier Computer Communications, 2009.