A User Authentication-Based Probabilistic Risk Approach for Wireless Sensor Networks

Youssou FAYE
Franche-Comte University
Laboratory LIFC
Besancon, France
yfaye@femto-st.fr

Ibrahima NIANG
Cheikh Anta Diop University
Dept Maths and Computer Science
Dakar, Senegal
iniang@ucad.sn

Herve GUYENNET
Franche-Comte University
Laboratory LIFC
Besancon, France
herve.guyennet@femto-st.fr

***Abstract*—Sensor nodes are low power devices which have limited computing resources. For various sensor network applications, providing a variety of security functions with limited energy resources and low power capabilities is a very big challenge. Recently, Vaidya *et al.* proposed an Improved Robust Dynamic User Authentication Scheme for Wireless Sensor Networks (WSNs) that allows legitimate users to query sensor data at every sensor node of the network. In this work, we show that, Vaidya *et al.*'s scheme suffers from the risk of forgery attacks and Denial-of-Service (DoS) attacks. To cope with them, we propose a new solution which is quite adequate for power and resource constrained sensor networks. The proposed scheme not only retains all the advantages in Vaidya *et al.*'s scheme but also protects against DoS and forgery attacks. After an evaluation of the energy cost based on the computational complexity, we use in our implementation the probability risk analysis owing to the DoS attack model to show to which level the proposed solution justifies the better energy consumption for a given network architecture.**

Keywords: Wireless Sensor Networks, authentication, password.

I. Introduction

A Wireless Sensor Network (WSN) is consisted of a large number of sensor devices working collaboratively to collect data about the monitored environment over a geographic area. In general, most queries in WSN applications are issued at the base stations or a Gateway node (GW). However, in real-time WSN applications, data are made available to the user on demand, data may no longer be accessed at the based station or the gateway node only, but also could be accessed anywhere from a sensor node in an ad hoc manner. In WSN critical applications, such as military surveillance, the collected data and secrets should protected by preventing unauthorized users from gaining the information. Then access control must be ensured to protect access to the critical data [2]. User Authentication (UA) is a basic used solution. Password-based authentication schemes [3,4,5,6,7] are the most widely used techniques for remote user authentication. UA has not been adequately addressed, due to sensor's limited processing capability, storage, and energy. Hence, WSNs need an authentication protocol with low expenses.

Vaidya *et al*. proposed an Improved Robust User Authentication Scheme for Wireless Sensor Networks [1]. This scheme comes with several advantages like low power energy consumption, providing protection against various attacks. However, this paper points out that Vaidya *et al*.'s scheme is insecure and cannot prevent from DoS attacks because it has the lack to check user's password in the login phase. It also cannot fully prevent from forgery attacks in the authentication phase because it suffers from the risk of a modified time delay. Therefore, we have proposed a scheme, whereby it does require mechanism to check user's password by login node (LN) and transmit time in a secure mode in order to overcome the risks of DoS and forgery attacks.

The rest of the paper is organized as follows. Section II presents related works. A review of Vaidya *et al*. [1] and some comments on this scheme are respectively presented in section III and IV. A new solution is proposed in section V. Security analysis of the new solution is provided in section VI. Section VII describes implementation, and finally, section VIII gives a brief conclusion.

II. Related Works

Authentication is a security service, a basic solution used for access control in WSNs. It means establishing a relation between a user or a sensor node and some identity which is an individuality property.

In User Authentication, the user sends his name and proofs of his identity to a sensor node, and the sensor should be able to decide whether or not the identity is valid and in fact belongs to the user of that name.

Traditional UA schemes [3,4,5,6,7] based on Lamport's scheme [8] are quite interesting to examine various works on smart cards, they are based on static login ID and use the techniques of Password-based authentication for remote UA, on which a verification table is no longer required in the remote system. Existing Password-based authentication schemes can be categorized into two types. One [4] uses weak-password and is difficult to apply in WSN because it is based on public-key cryptographic techniques. The other [3,5,6,7] uses strong-password and lead lighter computational because of using only one-way hash function and exclusive-OR operation (XOR). That's made it feasible to be adapted into the WSN environment. Several UA schemes and improvements have been proposed over the last few years. Das *et al*.[9]'s scheme for remote user authentication using smart card is based on a dynamic identifier (ID) and is claimed to be secure against ID-theft, and can resist the reply attacks,

978-1-4244-7803-3/12/$26.00 ©2012 IEEE

forgery attacks, guessing attacks, insider attacks and stolen verifier attacks. Lee et al. also proposed an improved UA scheme [10] with low computation cost based on one-way hash functions for smart cards. This scheme is claimed to be secure against forgery and replay attacks, and modified login message. Wong *et al*. [11] makes use of Lee's framework, but adapts it for a WSN environment. It uses basically one-way hash function and exclusive-OR operation to provide the dynamic UA. Based on Wong *et al*.'s scheme, Tseng *et al*. [13] proposed an improved user authentication scheme that points the weaknesses and also enhances the security of Wong *et al*.'s scheme.

Vaidya *et al*. [1] is a variation of strong-password based solution proposed by Wong *et al*. [11] and a modified version of their robust scheme[12]. Only four phases are used in this scheme, namely, Registration Phase(RP), Login Phase (LP), Authentication Phase (AP), and Password-changing phase (PP). Their proposed scheme comes with several advantages, provide protection against the replay attacks of login message and forgery attacks, but cannot fully prevent from various attacks. All phases are described in next section.

III. REVIEW OF VAIDYA *et AL.*'S PROTOCOL

Vaidya *et al*. [1] is divided into four phases. We briefly describe them in the following. The notations involved are listed in Table I.

TABLE I
NOTATIONS

Symbols	Description
UD	User's Device such PDA, PC
GW	Registration Sensor Gateway
LN	Sensor Login node
H( )	One-way hash function
$\oplus$	Exclusive-or (XOR) operation
$\|\|$	Concatenation
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
$\triangle$T	Allowed time interval for transmission delay

A. Registration Phase

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

Algorithm 1 : Steps of operations for Registration Phase

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

B. The Login Phase

In Login phase, the user computes A = H(vpw$\|$t) and 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$\geq\triangle$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.

Algorithm 2 : Steps of operations for Login Phase

LP1 - - UD : Computes A = H(vpw$\|$t);
LP2 - - UD $\longrightarrow$ LN : UID, A, t;
LP3 - - LN: **IF** UID exists on its table list
- **THEN** the corresponding X is known
- **ELSE** the login request is rejected;
- **IF** T_0 - t$\geq\triangle$T
- **THEN** the login request is rejected;
- **ELSE** retrieves A, computes C_K=(X $\oplus$A $\oplus$ T_0);
LP4 - - LN $\longrightarrow$ GW: UID,C_K,T_0,t;

C. The Authentication Phase

In Authentication phase, the GW checks whether or not UID and time t are valid. The login request is rejected if they are not. Otherwise, the GW verifies if T_1-T_0 $\geq$ $\triangle$T; T_0-t $\geq$ $\triangle$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,the GW computes V_M = H(X$\|$A'$\|$ T_1) and sends accept message (Acc_login, V_M, T_1) to the LN.

The LN computes V'_M and after verification of V_M =V'_M , it computes Y_K = H($V'_M\|$ T_2). The LN sends (Acc_login, Y_K, T_1, T_2) to the UD. Upon receiving the message at time T_3, the UD checks if T_1-T_0 $\geq$ $\triangle$T; T_0-t $\geq$ $\triangle$T. If the conditions are true, then the Acc_login message is rejected. Otherwise, the login node retrieves the corresponding A, performs $V"_M$ =H(X$\|$A$\|T_1$) and Y'_K = H($V"_M\|T_2$), and checks if Y_K =Y'_K. If it is true, then the UD starts obtaining data if the condition holds. Otherwise, accept login message is rejected.

D. The Password-Changing Phase

In the Password-changing phase,the UD changes his password PW to PW1. Then it computes vpw1 = H(PW1) and

Algorithm 3 : Steps of operations for Authentication Phase

AP1 - - GW: **IF** UID and t exists on its table list
- **THEN** retrieves parameters of dataset(UID, X, TS);
- **ELSE** the login request is rejected;
- **IF** T_1 - $T_0 \geq \triangle$T and T_0 - t$\geq \triangle$T
- **THEN** the login request is rejected;
- **ELSE** computes A' = H(vpw$\|$ t);
- computes C'_K = (X$\oplus$A'$\oplus$ T_0);
- **IF**$C'_K \neq C_K$
- **THEN** the login request is rejected;
- **ELSE** computes V_M = H(X$\|$A'$\|T_1$) and Store t;

AP2 - - GW $\longrightarrow$ LN: Access_login,V_M,T_1;

AP3 - - LN:**IF** T_2 - $T_1 \geq \triangle$T
- **THEN** the login request is rejected;
- **ELSE** computes V'_M = H(X$\|$A$\|T_1$);
- **IF** $V_M \neq V'_M$
- **THEN** the login request is rejected;
- **ELSE** computes Y_K=H($V'_M\|T_2$);

AP4 - - LN $\longrightarrow$UD:Acces_login,Y_K,T_1,T_2

AP5 - - UD:**IF** T_1 - T_0 $\geq \triangle$T and T_0 - t$\geq \triangle$T;
- **THEN** rejects the Acc_login message;
- **ELSE** computec $V"_M$ = H(X$\|$A$\|T_1$);
- computes Y'_K = H($V"_M\|T_2$);
- **IF** $Y_K \neq Y'_K$
- **THEN** rejects the Acc_login message;
- **ELSE** starts obtaining data;

sends the triple (UID, vpw, vpw1) to the GW. The GW checks UID and vpw. If both of them are true, GW updates its database. Then GW 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 check UID and update their databases.

Algorithm 4 : Steps of operations for The Password-Changing Phase

PP1 - - UD : computes Computes vpw1 = H(PW1);

PP2 - - UD $\longrightarrow$ GW : UID, vpw, vpw1;

PP3 - - GW: **IF** UID and vpw exist on its table list
- **THEN** Updates vpw, TS with vpw1 ,TS1 respectively;

PP4 - - GW $\longrightarrow$ UD: sends Succ_Change;

PP5 - - GW $\longrightarrow$LNs: send UID, TS1;

PP6 - - LN: **IF** UID exist on its table list
- **THEN** Updates TS with TS1;

IV. SECURITY WEAKNESS IN VAIDYA *et AL.*'S PROTOCOL

In this section, we point out an inherent design flaw in the login and authentication phases. We then demonstrate that Vaidya *et al*. [1] is being vulnerable to DoS and forgery attack, in violation of their security claims. Note that, during the login phase, there is one-hop communication between user's mobile device and the LN, and for the communication scenario between the LN and the gateway node, multiple hops may be required. DoS attacks can occur on two manners. First, the intruder can intercept or eavesdrop a valid UID and later try to submit it with a fake password. Then the LN checks only the UID, and after forwards a request for authentication to the GW. This fake query propagates in network before being reached the GW. Secondly, this scenario can happen when a valid user makes a mistake on entering his password. Since the most power consuming operation is wireless communication, the propagation of a fake query must restricted to a logarithmic part of the network.

Vaidya *et al.*[1] assume that an adversary captures LN to obtain (UID,X, TS) and eavesdrops (UID, A,t) to demonstrate that Wong *et al*.'s scheme cannot resist forgery attacks. With those assumptions, forgery attacks can occur on their scheme with following manner. Since timestamps are not transmitted over the network in encrypted mode and only expected time interval for transmission delay is verified by GW, the intruder can intercept two timestamps T_0 and t in login and authentication phase, and then computes T'_0=T_0+ξ ,t'=t+ξ with ξ a small number, it computes C'_K = H(X$\oplus$A$\oplus T'_0$) sends message (UID, $C'_K T'_0$,t'. As long as (T_1 - T'_0)$\leq \triangle$T and (T'_0-t')$\leq \triangle$T then it is passed.

V. PROPOSED SCHEME

In this section, we propose a new solution to solve the weaknesses in Vaidya *et al*. [1]. The flaws has introduced due forgery attacks and DoS attacks. The proposed scheme has same phases as Vaidya *et al.*'s scheme, only password-changing phase is not changed.

A. Registration Phase

In Vaidya *et al.*'s protocol, the user chooses a password PW, computes vpw=H(PW) and sends vpw for login. And in the rest of the communication handshakes, the PW is not used. It is not necessary to compute vpw=H(PW), because it is as vulnerable as the PW. The user can only choose a PW, submits it, and after the H(PW) is stored by GW and the LN.

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

Algorithm 5 : Steps of operations for Registration Phase

RP1 - - UD : chooses PW;

RP2 - - UD $\longrightarrow$ GW : UID, PW;

RP3 - - GW : computes X = H(UID $\|$ x);
-stores UID, H(PW), X, TS;

RP4 - - GW $\longrightarrow$ UD : Succ_Reg(X) ;

RP5 - - UD : stores X;

RP5 - - GW $\longrightarrow$LNs : UID, X, TS;

RP6 - - LN: stores UID, X, H(PW),TS;

B. The Login Phase

In Login phase, the user computes A= H(H(PW)‖t) and 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 . The login request is rejected if it is not. The LN computes A'= H(H(PW)‖t), checks if A=A' and T_0 - t $\geq\triangle$T (the password is valide if A=A') . The login request is rejected if it is not. Otherwise, the login node retrieves the corresponding A and computes C_K = (X$\oplus$A$\oplus T_0$). Computes t'=H^2(PW)$\oplus$t. The expression H^n(PW) denotes the application of n cascade hash operations starting from PW. That is, H^n(PW)=H(H^{n-1}(PW)).

Algorithm 6 : Steps of operations for Login Phase

LP1 - - UD : computes A = H(H(PW)‖t);
LP2 - - UD $\longrightarrow$ LN : UID, A, t;
LP3 - - LN: **IF** UID is not valide
- **THEN** the login request is rejected;
- **ELSE** computes A' = H(H(PW)‖t);
- **IF** A$\neq$A'
- **THEN** the login request is rejected;
- **ELSE IF** T_0 - t$\geq\triangle$T
- **THEN** the login request is rejected;
- **ELSE** retrieves the corresponding A;
- computes C_K=(X $\oplus$A $\oplus$ T_0);
- computes t'=H^2(PW)$\oplus$t;

LP4 - - LN $\longrightarrow$ GW:UID,C_K,T_0,t';

C. The Authentication Phase

In Authentication phase, the GW checks whether or not UID and t are valid. The login request is rejected if it is not. Otherwise, the GW Computes t= t'$\oplus H^2$(PW), checks if T_1 - $T_0\geq\triangle$T ; T_0 - t$\geq\triangle$T. If the condition is satisfied, then the login request is considered as a replay message and is rejected. On the other hand, the GW retrieves the corresponding H(PW) and A, computes A' = H(H(PW)‖t) and C'_K = (X$\oplus$A'$\oplus$ T_0). The login request is rejected if $C_K\neq C'_K$. Otherwise, the GW computes V_M = H(X‖A'‖T_1) and sends accept message (Acc_login, V_M, T_1) to the login node. The LN computes V'_M, and after verification of V_M = V'_M , it computes Y_K = H(V'_M‖T_2). The LN sends (Acc_login, Y_K, T_1, T_2) to the UD. Upon receiving the message at time T_3, the UD checks if T_1 - $T_0\geq\triangle$T; T_0 - t$\geq\triangle$T. If the conditions are true, then the Acc_login message is rejected. Otherwise, the LN retrieves the corresponding A, performs $V"_M$ = H(X‖A‖T_1) and Y'_K = H($V"_M$‖T_2), and checks if Y_K =Y'_K. If the condition holds, then the UD starts obtaining data . Otherwise, accept Acc_login message is rejected.

D. The Password-Changing Phase

The password-changing phase is the same as Vaidya *et al* [1].

Algorithm 7 : Steps of operations for Authentication Phase

AP1 - - GW: **IF** UID and t are valid
- **THEN** retrieves parameters of dataset(UID, X, TS, H(PW));
- compute t=t'$\oplus H^2$(PW);
- **ELSE** the login request is rejected;
- **IF** T_1 - $T_0\geq\triangle$T and T_0 - t$\geq\triangle$T
- **THEN** the login request is rejected;
- **ELSE** computes A' = H(H(PW)‖ t);
- computes C'_K = (X$\oplus$A'$\oplus$ T_0);
- **IF**$C'_K\neq C_K$
- **THEN** the login request is rejected;
- **ELSE** computes V_M = H(X‖A'‖T_1);
- stores t;

AP2 - - GW $\longrightarrow$ LN: Access_login,V_M,T_1;
AP3 - - LN: **IF** T_2 - $T_1\geq\triangle$T
- **THEN** the login request is rejected;
- **ELSE** computes V'_M = H(X‖A‖T_1);
- **IF** $V_M\neq V'_M$
- **THEN** the login request is rejected;
- **ELSE** computes Y_K=H(V'_M‖T_2);

AP4 - - LN $\longrightarrow$UD: Acces_login,Y_K,T_1,T_2
AP5 - - UD: **IF** T_1 - T_0 $\geq\triangle$T and T_0 - t$\geq\triangle$T;
- **THEN** rejects the Acc_login message;
- **ELSE** computes $V"_M$ = H(X‖A‖T_1);
- computes Y'_K = H($V"_M$‖T_2);
- **IF** $Y_K\neq Y'_K$
- **THEN** rejects the Acc_login message;
- **ELSE** starts obtaining data;

VI. ANALYSIS OF OUR SCHEME

In this section, through analysis based evaluations, we show that the proposed scheme overcomes the security problems. In addition, we will provide a comparative study with some existing solutions.

A. Security Analysis

DoS attacks: our scheme can protect against DoS attacks because it allows LN to check user's password in login phase. Since the LN stocks H(PW), after receiving the login message (UID, A,t), it can compute A'=H(H(PW)‖t). If A'=A then the password is correct, else the login message is rejected.

Forgery attacks: our scheme can also protect against the forgery attack because time t is transmitting in a secure mode. In Vaidya *et al*.'s scheme, the login message is not sent via a secure channel between the user and the LN, the attacker can eavesdrop login message (UID,A,t) and modify the times T_0 and t. In our solution, to secure the time t in the login message between the LN and the GW, the LN computes a fake time t'=H^2(PW)$\oplus$t and transmits (UID,C_K,T_0,t') to GW. After receiving this message, since H^2(PW)$\oplus$t$\oplus H^2$(PW) = t, the GW computes t = t'$\oplus H^2$(PW) to find t.

B. Overhead Cost Comparisons

Table II summarizes the comparisons of our scheme with Vaidya *et al*.'s schemes and other solutions.

TABLE II
OVERHEAD COST COMPARISON.

Protocols	Total Cost Overhead
Wong et al.'s Scheme [11]	$7T_H$+$4T_{XOR}$+$3C_{MH}$
Tseng et al.'s Scheme[13]	$5T_H$+$4T_{XOR}$+$3C_{MH}$
Vaidya et al.'s Robust Scheme [12]	$8T_H$+$4T_{XOR}$+$3C_{MH}$
Vaidya et al.'s Improved Robust Scheme[1]	$11T_H$+$4T_{XOR}$+$3C_{MH}$
Proposed Scheme	$15T_H$+$7T_{XOR}$+$3C_{MH}$

T_H: the time for performing a one-way hash function *h()*.
T_{XOR} : the time for performing an XOR operation.
C_{MH} : the delay time for the communication taken place between the login-node and the GW-node in multi-hops.

We can see from Table II that the total overhead cost of the proposed scheme is slightly higher than Vaidya *et al*. Improved Robust Scheme[1]. The additional computational cost of our solution is $4T_H$ operations and $3T_{XOR}$ operations. Note that in [14] it is mentioned that the time for computing XOR operations is much smaller than T_H. So, our proposed scheme has little higher overhead cost than Vaidya *et al*.'s schemes, however it provides better security. Furthermore, if we consider query with valid UID and fake password sent by an intruder or a legal user, for Vaidya *et al.*'s scheme, this false query is propagated up to GW by sensor nodes, while for our solution, its propagation is restricted. Table III summarizes the comparisons of our scheme with Vaidya *et al.*'s schemes. We can see from Table III that the total overhead cost of the proposed scheme is less than those of Vaidya *et al.*'s previously schemes. And this will increase with number of hops between the LN and the GW.

TABLE III
OVERHEAD COST COMPARISON.

Protocols	Total Cost Overhead
Vaidya et al.'s Robust scheme [12]	$4T_H$+$2T_{XOR}$+$2C_{MH}$
Vaidya et al.'s Improved Robust scheme[1]	$4T_H$+$2T_{XOR}$+$2C_{MH}$
Proposed Scheme	$3T_H$

VII. IMPLEMENTATION

We have implemented the proposed solution and Vaidya *et al.* Improved Robust Scheme[1] with TinyOS and tested them using MicaZ based Avrora. The goal of our implementation is to measure energy consumption according to the number of hops between the LN and the GW and also the probability of a fake password.

At the first step, we evaluate energy of both schemes based on Table II where no fake query is considered. For each data fields (UID,A, C_k etc.) we use 4 bytes. We use the implementation of PolyR universal function as a TinyOS interface. PolyR is a Fast Universal Hashing with Small Keys and no preprocessing. Its implementation follows the original paper of Ted *et al.*[15]. Since our scheme uses more operations, in

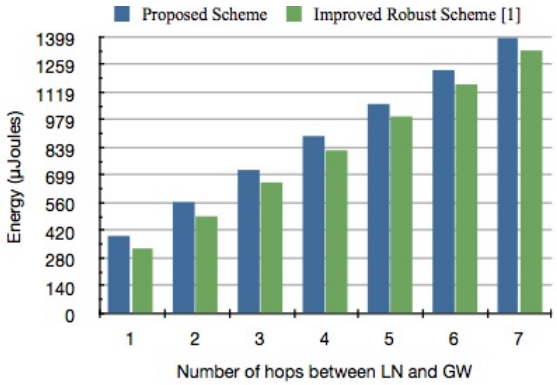

Fig. 1. **Energy Consumption based on Table II**.

Figure 1, we can see that our scheme consumes more energy than Vaidya *et al.*'s scheme.

At the second step, we study the energy consumption with the propagation of fake query which has been submitted by an intruder or a legal user who makes a mistake on entering its password. In **Figure 2**, we can see that the energy consumption of our scheme is constant and less than Vaidya *et al.*[1] which increases with the number of hops between the LN and GW.

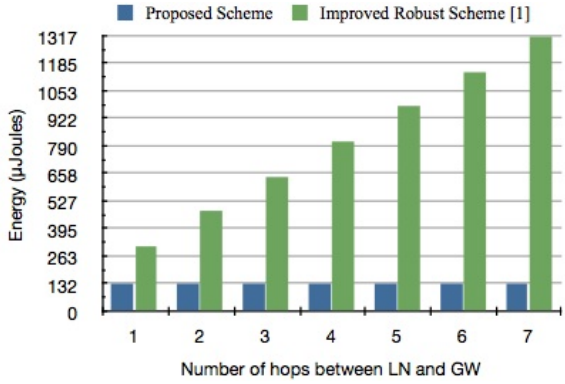

Fig. 2. **Energy Consumption based on Table III**.

At the third step, we introduce the probability of a fake query. In the following, we will analytically determine the energy consumption of each scheme based on the probability of fake password. Variables used for analysis are summarized in Table IV. According to a uniform probability distribution

TABLE IV
VARIABLES USED IN THE ANALYSIS.

Meaning of the variable	Variable
Energy consumption without fake password (Figure1)	E_v
Energy consumption with fake password (Figure2)	E_w
Energy consumption with probability P_i	E_i
Probability of fake password	P_i

P_i of a fake password, in the next formula, E_i is energy consumption for a probability P_i.

$$E_i = P_i * E_w + (1\text{-}P_i) * E_v$$

Based on this formula and the number of hops between the login node and the gateway node, our next task is to find the

probability from what the proposed scheme has better energy consumption. The results of energy evaluation based on the apposite formula are presented in **Figure 3** for one hop, **Figure 4** for two hops and **Figure 5** for four hops.

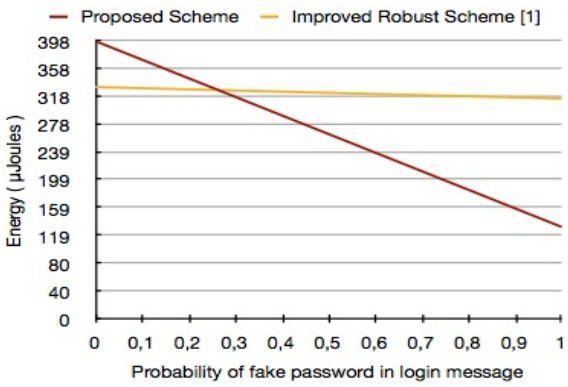

Fig. 3. **Energy Consumption for 1 hop between LN and GW**.

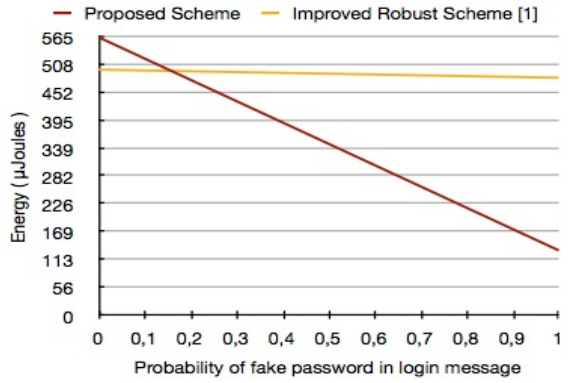

Fig. 4. **Energy Consumption for 2 hops between LN and GW**.

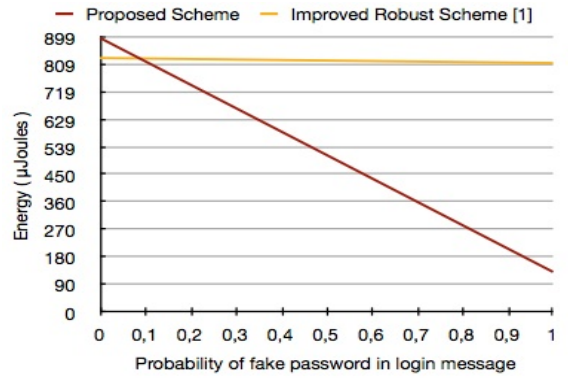

Fig. 5. **Energy Consumption for 4 hops between LN and GW**:

We found out that our proposed scheme does bring significant improvements, the best results are reached on $P_i \leq 0{,}3$ for one hop, $P_i = \leq 0{,}13$ for two hops and $P_i \leq 0{,}09$ for four hops.

VIII. Conclusion

In this paper, we proposed a new solution based on risk analysis of Vaidya *et al*. [1]. Our solution retains all the advantages in Vaidya *et al*.'s scheme and overcomes the problems of DoS attacks and forgery attacks. On the one hand, in a riskless situation (probability of risk equal 0), the proposed solution implies a better security with an additional computational cost of $4T_H$ and $3T_{XOR}$ operations. On the other hand, through analysis and simulation based evaluations, we show that the proposed solution has better energy consumption. It also seems to be promising, as it decreases the number of sent messages in the network, and therefore, saves energy. For a given network architecture based on the number of hops between the LN and GW node, we show the probability to which each solution has better energy consumption.

References

[1] Binod Vaidya, Min Chen and Joel J. P. C. ,Rodrigues, Improved Robust User Authentication Scheme for Wireless Sensor Networks, Wireless Communication and Sensor Networks (WCSN), 2009 Fifth IEEE Conference: December 15-19

[2] Y. Faye, I. Niang and T. Noêl. A Survey of Access Control Schemes in Wireless Sensor Networks. World Academy of Science, Engineering and Technology, Issue 59: 2011, Paris, France, Pages 814-823, November 2011.

[3] A. K. Awasthi, and S. Lal, A remote user authentication scheme using smart cards with Forward Secrecy, IEEE Transactions on Consumer Electronics, vol.49, no.4, pp.1246-1248, Nov. 2003.

[4] M. S. Hwang, C. C. Chang, and K. F. Hwang, An E1Gamal-like cryptosystem for enciphering large messages, IEEE Trans .on Knowledge and Data Engineering, vol.14, no.2, pp.445-446, 2002.

[5] C. C. Lee, L. H. Li, and M. S. Hwang, A remote user authentication scheme using hash functions, ACM Operating Systems Review, vol.36, no.4, pp.23-29, 2002.

[6] J. J. Shen, C. W. Lin, and M. S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. on Consumer Electron., vol.49, no.2, pp.414-416, May 2003.

[7] H. M. Sun, An Efficient remote user authentication scheme using smart cards, IEEE Trans. on Consumer Electron., vol. 46, no. 4, pp. 958-961, Nov. 2000.

[8] L. Lamport, Password authentication with insecure communication, Communications of the ACM, vol.24, no.11, pp.770-772, 1981.

[9] M.L. Das, A. Saxena, and V.P. Gulati, A Dynamic ID-based Remote User Authentication Scheme, IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, 2004.

[10] C.Y. Lee, C.H. Lin, and C.C. Chang, An Improved Low Communication Cost User Authentication Scheme for Mobile Communication, Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications (AINA 2005), Taiwan, March 2005.

[11] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, 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), vol. 1, Jun. 2006, pp. 244-251.

[12] B Vaidya, J.S. Silva, J.J. Rodrigues, Robust Dynamic User Authentication Scheme for Wireless Sensor Networks, In Proc. of the 5th ACM Symposium on QoS and Security for wireless and mobile networks (Q2SWinet 2009), Tenerife, Spain, Oct. 2009, pp 88-91.

[13] 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 (GLOBECOM07), Nov. 2007;986-990.

[14] Hui-Feng Huang,Kuo-Ching Liu,A New Dynamic Access Control in Wireless Sensor Networks, 2008 IEEE Asia-Pacific Services Computing Conference, DOI 10.1109/APSCC.2008.116

[15] Ted Krovetz, Phillip Rogaway,Fast Universal Hashing with Small Keys and No Preprocessing: The PolyR Construction, D. Won (Ed.): ICISC 2000, LNCS 2015, pp. 73-89, 2001. Springer-Verlag Berlin Heidelberg