Energy Efficient Authentication Scheme for Industrial Smart Grid Environments

D. Password-change phase

To enhance the security strength, a proposed scheme allows flexibility of password change. Before password change, it is important for node devices to prove their genuineness to serve through successful authentication verification (See Fig. 1). This is process only done by the expert of company if any problem is noted from client, who are currently using it. The password change phase details are as follows:

Step 1. $\boldsymbol{U_i} \rightarrow \mathbf{TS}$: $< I_i, X_i, Y_i, P_{ke_i} >$. The legitimated node (U_i) chooses random ephemeral secrete $x_{i1} \in Z_p$, and computes challenges $X_i = x_{i1}.G$ using ECC point multiplication, hides x_{i1} inside $Y_i = x_{i1} \oplus P_y\ h1(x_{i1}.P_{ks})$, and finally sends an authentication request containing challenges $< I_i, X_i, Y_i, P_{ke_i} >$ to TS in the SG network through a open channel with whom they want to communicate.

Step 2. $\mathbf{TS} \rightarrow\ \boldsymbol{U_i}$: $< X_j, Y_j\ >$. After receiving an authentication request, the TS search out I_i in database check $P_{ke_i}(Recived) = ?\,P_{ke_i}$(Available). Recomputes $P_{xi} = P'_{xi} \oplus \mathrm{s} \oplus I_i \oplus I_{TS}$, $P_{yi} = P'_{yi} \oplus P'_{xi} \oplus \mathrm{s} \oplus I_i \oplus I_{TS}$ and checks verifies it (i.e., $Y_i.G =?\ X_i \oplus P_{yi}\ h1(X_i.\mathrm{s})$). Unsuccessful deduction from both sides leads to session termination. Otherwise, proceed to the next step then legitimated node (U_j) chooses random ephemeral secrete $x_{j1} \in Z_p$, and computes challenges $X_j = x_{j1}.G$ using ECC point multiplication, hides x_{j1} inside $Y_j = x_{j1} \oplus P_{yi}\ h1\left(I_i, x_{j1}.P_{ke_i}\right)$, and finally sends response challenges $< X_j, Y_j >$ to an authentication request of U_i.

Step 3. Session key $\left(S_K = x_{i1}.X_j.Psw_i.P_{ks}\right)$ computation.

After receiving a challenge, node (U_i) recompute and verify the challenge (i.e., $Y_j.G =?\ X_j \oplus P_y\ h1\left(I_i,\ X_j.Psw_i\right)$ and then compute the session key $(S_K = x_{i1}.X_j.Psw_i.P_{ks})$. Then $\boldsymbol{U_i}$ choose a new password and repeat the same procedure mentioned in the registration phase III.B and used session (S_K) to encrypt communication over public channel.

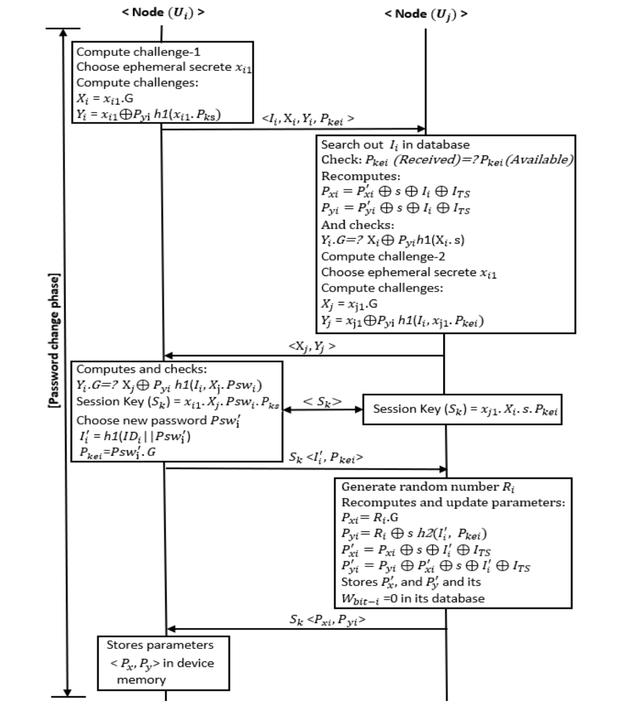
< Node (U_i) >
< Node (U_j) >
[Password change phase]
Compute challenge-1
Choose ephemeral secrete x_{i1}
Compute challenges:
$X_i = x_{i1}.G$
$Y_i = x_{i1} \oplus P_{yi}\ h1(x_{i1}.P_{ks})$
$<I_i, X_i, Y_i, P_{kei}>$
Search out I_i in database
Check: P_{kei} (Received)=? P_{kei} (Available)
Recomputes:
$P_{xi} = P'_{xi} \oplus s \oplus I_i \oplus I_{TS}$
$P_{yi} = P'_{yi} \oplus s \oplus I_i \oplus I_{TS}$
And checks:
$Y_i.G=?\ X_i \oplus P_{yi} h1(X_i.s)$
Compute challenge-2
Choose ephemeral secrete x_{i1}
Compute challenges:
$X_j = x_{j1}.G$
$Y_j = x_{j1} \oplus P_{yi}\ h1(I_i, x_{j1}.P_{kei})$
$<X_j, Y_j>$
Computes and checks:
$Y_i.G=?\ X_j \oplus P_{yi}\ h1(I_i, X_j.Psw_i)$
Session Key $(S_k) = x_{i1}.X_j.Psw_i.P_{ks}$
Choose new password Psw'_i
$I'_i = h1(ID_i||Psw'_i)$
$P_{kei} = Psw'_i.G$
$< S_k >$
Session Key $(S_k) = x_{j1}.X_i.s.P_{kei}$
$S_k <I'_i, P_{kei}>$
Generate random number R_i
Recomputes and update parameters:
$P_{xi} = R_i.G$
$P_{yi} = R_i \oplus s\ h2(I'_i,\ P_{kei})$
$P'_{xi} = P_{xi} \oplus s \oplus I'_i \oplus I_{TS}$
$P'_{yi} = P_{yi} \oplus P'_{xi} \oplus s \oplus I'_i \oplus I_{TS}$
Stores P'_x, and P'_y and its
W_{bit-i} =0 in its database
$S_k <P_{xi}, P_{yi}>$
Stores parameters
$< P_x, P_y >$ in device
memory

Fig.1. Password-change phase