Reply to the Reviewer’s Comments

Title: "A Lightweight Dynamic Pseudonym Identity Based Authentication and Key Agreement Scheme Using Wireless Sensor Networks for Agriculture Monitoring"

Authors: Meriske Chen, Tian-Fu Lee, Jiann-I Pan

Reference No.: sensors-415828

Summary of the changes in response to the review of ID: sensors-415828

We would like to thank the editor and the anonymous reviewers for your very helpful and valuable comments on our manuscript entitled "A Lightweight Dynamic Pseudonym Identity Based Authentication and Key Agreement Scheme Using Wireless Sensor Networks for Agriculture Monitoring". We have revised the manuscript according to the reviewers’ comments. The main changes in response to the reviewing results are listed below.

1. We have added more descriptions and explanations to explain the proposed scheme in this version according to the reviewers’ comments.

2. We have modified our title for Sec. 2 and restructured our manuscript according to the reviewers’ comments.

3. The typo errors and mistakes have been corrected and revised in this version according to the reviewers’ comments.

Comments and Suggestions for Authors

Reviewer 1

This paper firstly analyzed an authentication and key agreement scheme for wireless sensor network (WSN) based agriculture monitoring, which is presented by Ali et al. The authors discovered that Ali et al.’s scheme has many flaws and vulnerable to many attacks (including the insider). In order to enhance the security of Ali et al.’s scheme, secondly, the authors proposed a lightweight dynamic identity based user authentication scheme for WSN based agriculture monitoring.

The paper is well organized and well written. Few comments:

(i) Recently, many of user authentication schemes have been studied and proposed in generic WSN. How these two schemes (i.e., Ali et al. and the proposed scheme) are different than others. Does agriculture application requires different security...
requirements, which cannot be fulfilled by the generic proposed schemes?

Answer: We thank the reviewer for this constructive suggestion. When we see how importance the agriculture for everyone, we know that we need to give a study that focus on it. Other general schemes for WSNs may not necessarily accordance with agriculture monitoring necessities. For example, even for the organization structures such as entities (user, sensor nodes, gateway nodes, cluster head, etc.) can be different with the general schemes because of its different designation purposes. Ali, et al. are the first authors whose can see these importance and then designed a special scheme for agriculture monitoring using WSNs. Unfortunately, their scheme suffered from major security weaknesses. Our study mentioned their weaknesses and proposed an improved scheme which is more secure and more efficient a lot. The related descriptions are shown on Pages 1-2, Sec. 1, Paragraphs 1 and 2.

(ii) In my opinion, considering the insider attack – the scheme proposed by Ali et al.s is indeed vulnerable to sensor node impersonation attack, perfect forward secrecy, and violation of session key security and user anonymity.

Answer: We thank the reviewer for this constructive suggestion.

(iii) In the proposed scheme (page 9, Section IV), many assumptions are not clear, e.g., (i) how Ai is shared between the user and the base station (BS), at first place. (ii) Who is the system administrator (i.e., BS or some another entity) and how the keys are being distributed to the entities. Not enough clear.

(iii.i) “how Ai is shared between the user and the base station (BS), at first place.”

Answer: We thank the reviewer for this constructive suggestion. There are 2 parts where Ai is shared with BS.

- The first part, Ai is shared with BS in user registration phase (as shown in Figure 5) and Section 4.1, Step 1, through this message: \{ID_i, RPW_i, A_i\}. However, in our Section 4.1, Step 1, we just found that we did not put Ai into this statement: “Now, U_i sends \{ID_i, RPW_i\} to BS via trustworthy channel.”. We added A_i to \{ID_i, RPW_i\}. Now, in Section 4.1, Step 1 become “Now, U_i sends \{ID_i, RPW_i, A_i\} to BS via trustworthy channel.”.
- The second part, Ai is shared with BS during login phase through this message: \{A_i, DID_i, T_1, M_1, ID_{SN_j}, ID_{GW_N_j}\}, as shown in Figure 6 and Section 4.2, Step 2. BS never store Ai in its database. Ai always be declared openly during the login phase. The function of Ai is to make sure that Ui holds a legal shared key with BS,
where the shared key between them is $h(A_i \| X)$.

(iii.ii) “Who is the system administrator and how the keys are being distributed to the entities.”

**Answer:** We thank the reviewer for this constructive suggestion.
- The system administrator is the base station (BS). To make it clear, we added some information to make it clearer for reader.
- Which part about the keys that are not clearly distributed?

(iv) In the proposed scheme, the message $M_5$ (refer to authentication and key agreement phase: Step 2) is computed via $RBS \oplus h(h(IDSN_i \| X) \| T_3)$ at the BS. Now, using $M_5$, the SN derives $RBS^* = M_5 \oplus h(RJ_i \| T_3)$, refer to authentication and key agreement phase: Step 5. I am wondering how $RBS$ will be derived from $M_5$, since these two expressions are different?

**Answer:** We thank the reviewer for this constructive suggestion.
- First, we need to see the system setup phase in section 2.1, where $R_{I_j}$ is a shared key between BS and SN, and $R_{I_j} = h(ID_{SN} \| X)$.
- Now, we go to section 4.3, step 2, where $M_5 = R_{BS} \oplus h(h(ID_{SN} \| X) \| T_3)$ and section 4.3, step 5, where $R_{BS}^* = M_5 \oplus h(RI_j \| T_3)$.
- Since $R_{I_j} = h(ID_{SN} \| X)$, then $R_{BS}^* = M_5 \oplus h(RI_j \| T_3)$ equals with $R_{BS}^* = M_5 \oplus h(h(ID_{SN} \| X) \| T_3)$.

Now, we can clearly see that SN can derive $R_{BS}$ from $M_5$. The descriptions are shown on Page 4, Sec. 2.1.

(v) Regarding the security analysis, as the BAN logic itself has many inherent issues, this reviewer would like to recommend to use other software-based tools, e.g., Tamarin prover tool, or Scyther, for the formal security verification.

**Answer:** We thank the reviewer for this constructive suggestion. Indeed, the BAN logic cannot completely consider security requirements. We thus try to adopt the BAN logic analysis in Sec 4.1 and heuristic security analyses in Sec 4.2 to have complete security requirements. We leave this part for future work, as we need more time to apply such software-based tools.

(vi) In the informal analysis – what kind of attack model is being used, not enough clear. More importantly, how the new proposed scheme is secure against the insider attack, the authors should provide more justifications.

**Answer:** We thank the reviewer for this constructive suggestion. We have revised the
descriptions according to the reviewer’s comments. The new proposed scheme has already mentioned in Section 3 about how the proposed scheme is secure against the insider attack and by then eliminates the sensor node impersonation attack, perfect forward secrecy and violation of user anonymity (lines 268-271 in Section 3). Additionally, we also provide more justifications about how the new proposed scheme is secure against the insider attack in Section 4.2.11.