Author Response

Dear Editors/Reviewers,

On behalf of my co-authors, we thank you very much for giving us an opportunity to revise our manuscript. We truly appreciate the positive and constructive comments and suggestions given by the editors and reviewers. After carefully studying the comments, we have made the corresponding modifications which are listed in the following with label "Author_Response" (after each reviewer's comment starting with "Comment"). Furthermore, we also corrected the typos and grammar errors in the paper.

1 Reviewer 1

- Comment 1.1: Please cite the following important related papers.

- Author_Response 1.1: We thank the referee 1 for recommending these important papers. We cited these papers in Section 2 (Related Work).

- Comment 1.2: I suggest you should insert your contributions in Introduction.

- Author_Response 1.2: We thank the referee 1 for this good suggestion. We re-organized the Section 1 (Introduction) to include a specific paragraph about our contributions.

2 Reviewer 2

- Comment 2.1: Section "Introduction" mixes the problem motivation and description together with related works and details of the solution. In particular, the paper results (page 3) make reference to concepts such as DAC and "synchronized state" that, at that point of the paper, have not been introduced even intuitively.

- Author_Response 2.1: We particular re-organized the Section 1 (Introduction). In order to make the introduction to be more intuitive, we first removed the concrete notations regarding the protocol specification. Also, we further divided the contents to five parts, i.e., background, communication model, motivating problems, our contributions, main challenges and solutions.

- Comment 2.2: Furthermore, Section "Introduction" mentions implementation details, e.g., ss_i, $ss_{i,1}$, $ss_{i,2}$, that are totally inadequate at that stage. The net result is that Introduction is hardly comprehensible.

- Author_Response 2.2: We removed those concrete implementation details. A high-level overview of our construction is now given in the introduction.

- Comment 2.3: The main problem is that the reader is overwhelmed by lot of formalism (Section 4 and Section 5), but the paper completely fails to define and convey, at least intuitively, the main concepts at the basis of the proposed solution.

- Author_Response 2.3: We thank the referee 1 for pointing out the organization issues. In Section 4 (Security Model), we added a few sentences to explain the execution environment, adversarial model, and other important elements in our model. In Section 5, we particularly added a paragraph to introduce the concepts of our protocol construction from the perspectives of (i) structure of dynamic authentication credential (DAC), (ii) ephemeral authentication and encryption keys, (iii) DAC Update-key, and (iv) DAC update strategies.

- Comment 2.4: Therefore, I recommend to re-organize the paper, possibly moving the formal part into an appendix, and trying to introduce concepts before using them.

- Author_Response 2.4: We moved some remarks about the notations and other supplementary descriptions into Appendix A. The reader can look up the Table 8 for the descriptions of notations. Table 9 and Figure 7 can help a reader to better understand why our DAC update strategies work. In Section 5 (The Proposed AKA Protocol), We have modified the text in Section, to better explain the underlying concept of our protocol.

- Comment 2.5: Page 5, line 44: what do you mean by "not completely identical"?

- Author_Response 2.5: We removed such note since it is unclear without the context of our protocol. Instead, we explain this issue in Section 5.

- Comment 2.6: at page 9, line 41, authors say "The value u (cf. v) is used to store the index which indicates the current synchronized sub dynamic authentication credential (sub-DAC)". But, authors have not defined what a "synchronized sub dynamic DAC" is.

- Author_Response 2.6: We now use the term "sub-key" instead of sub-DAC (which is unclear) to describe the structure of the DAC. Basically, each DAC in our system consists of two sub-keys.

- Comment 2.7: Page 7, lines 13-14: the sentence does not parse.

- Author_Response 2.7: Thanks for pointing out this problem. We rephrased that sentence to make it to be more clear. Specifically, we changed the sentence from the original one:
"Let $\mathsf{pf} : (\mathcal{ID}_i, s, \mathsf{pid}^s_{\mathcal{ID}_i}, T^s_{\mathcal{ID}_i}) \rightarrow (\mathcal{ID}_j, t)$ be a partner function which is a map on a given execution states of $\Pi^s_{\mathcal{ID}_i}$ points to its partner oracle $\Pi^t_{\mathcal{ID}_j}$, where $\mathcal{ID}_j \in \mathsf{pid}^s_{\mathcal{ID}_i}$ and $t \in [d]$"
, to be the following one:
"Let $\mathsf{pf} : (\mathcal{ID}_i, s, \mathsf{pid}^s_{\mathcal{ID}_i}, T^s_{\mathcal{ID}_i}) \rightarrow (\mathcal{ID}_j, t)$ be a partner function; the inputs it requires are the identity $\mathcal{ID}_i$, the index s, and the internal states $\mathsf{pid}^s_{\mathcal{ID}_i}$ and $T^s_{\mathcal{ID}_i}$ of the oracle $\Pi^s_{\mathcal{ID}_i}$; its output is a tuple $(\mathcal{ID}_j, t)$ pointing to the partner oracle of $\Pi^s_{\mathcal{ID}_i}$, where $\mathcal{ID}_j \in \mathsf{pid}^s_{\mathcal{ID}_i}$ and $t \in [d]$."

- Comment 2.8: Page 9, line 7 and 18: what do you mean by "secure channel"?

- Author_Response 2.8: We added the description and assumptions about the secure channel. We assume that the secure channel satisfies confidentiality, authenticity and integrity. Such secure channel can be established based on out-of-band mechanisms, i.e., the user runs the registration procedure with the gateway node in a trustworthy environment that is isolated from the adversaries.

- Comment 2.9: Page 9, line 13: ss_i comes out of the blue. Are you sure that in $ss^{\mathsf{GW}}_{j,i}$ the superscript GW is correct?

- Author_Response 2.9: ss_i and ss^{GW}_i are basically pre-shared symmetric key (DAC) at the setup phase. We use a superscript 'GW' to denote the DAC that is initialized at the gateway node.

- Comment 2.10: Page 9, line 29: what does "[2]" mean?

- Author_Response 2.10: As described in Section 3 of the paper, $[n] = \{1, 2, \ldots, n\}$ denotes a set of natural numbers ranging from 1 to n. Therefore, the notation "[2]" which appears in any equation within this paper denotes $\{1, 2\}$.

- Comment 2.10: Page 9, line 40: which valued does u get?

- Author_Response 2.10: The value of u determined by the value of the index τ which indicates the authentication message $A_{i,\tau}$ that passes the verification, where $\tau \in [2]$.

3 Reviewer 3

- Comment 3.1: However, the reviewer has a major concern with regard to the 2nd stage of the protocol (i.e., sensor registration phase), in which sensor registrations are initiated by a gateway and the authentication of a gateway's identity is missing. Considering an attack model where an

adversary impersonates a gateway in this stage. Based on the current proposal, the fraud gateway (owned by the adversary) can randomly assign an SID to a targeted sensor. It is then fairly easy for the attacker to register herself to the fraud gateway and retrieve information from the targeted sensor. All the rest stages (stage 3 and stage 4) can be bypassed.

- Author_Response 3.1: We thank the referee 3 for pointing out this threat. In our proposal, we assume that gateway node is totally honest (and not corrupted by any adversary), and trusted by all other parties. This assumption is also commonly used by the similar authentication protocols in WSNs, e.g.,[9,15,33,52]. Hence, the initial authentication key and the identity of a sensor is sent by the gateway node via an existing secure (trustworthy) channel that is established via out-of-band mechanisms (isolated from adversaries). The secure channel can be established for example via an isolated cable that is directly connected between the honest gateway node and the registering sensor. We do not consider such strong attack model that the gateway node is compromised or controlled by the adversary in our paper for simplicity. We just focus on introducing a new efficient way to achieve PFS. Nevertheless, our proposed protocol can prevent the attacker from impersonating other uncorrupted sensors using a corrupted sensor. But it might be interesting to proposed a strongly secure AKA protocol that can resist such insider threat as a future work.

• Comment 3.2: The reviewer is also curious about the motivation of establishing a direct secure channel between a user and a sensor node. In the examined network model, because both sensors and users have connections to the gateway, it is possible to let the gateway authenticate a user. After the user is authenticated, the gateway pulls the info from the requested sensor and forward that info to the user. Compared with the authors' proposal, authentication at the gateway simplifies the protocol in this network model.

- Author_Response 3.2: In our motivated communication model (as shown in Fig. 1), the user's device (e.g., a smart card) is directly connected to a sensor, and the sensor relays the messages between the gateway node and the user's device. This model is suitable for all applications where the user's device cannot directly or efficiently connect to the remote gateway node (e.g., at a place without 4G). One application based on this communication model is the on-site sensor operation or data acquisition. Besides the data from the sensor, the sensor also may receive critical information (e.g., new configuration profile) from the user's device. In this case, it is more efficient to directly exchange the messages (which may be huge data) between the sensor and the user's device, without relying on the gateway node. For example, the sensor may provide a human machine interface and a card reader for the user. And the user who wants to control the sensor may need to insert its smart card and run the AKA protocol with the help of the remote gateway node, since the user's smart card and the

sensor share no key. Such direct secure channel between a user and a sensor node is also necessary and convenient when a mobile user (e.g., a boat in the sea without satellite communication) wants to securely join an existing ad-hoc wireless sensor network (established by other boats). Similar communication scenario has also been widely considered in references, e.g.,[9,15,33,52]. Besides, privacy could be a concern to the users. The user may not want the gateway node to learn any information (incl. the size) about the messages transmitted between the user and the sensor. Different communication models would yield different (and even incomparable) protocols. If both the user and the sensor can efficiently connect to the gateway node, e.g., via Internet, then the communication cost might be reduced. But this kind of communication model is distinct to the ours. As a future work, one can apply our construction idea (on achieving PFS) to design new AKA protocols for other communication models.