Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks (Appendix File)

Chenyu Wang, Ding Wang, Yi Tu, Guoai Xu, Huaxiong Wang

Abstract—This appendix file consists of two parts. Appendix A takes Li et al.’s scheme as an example to show a viable way to follow our proposed suggestions in Section 5. Appendix B extends the discussion about the comparison results in Table 5, with a focus on node capture attacks.

Index Terms—Appendix file.

APPENDIX A: A CONCRETE EXAMPLE TO ILLUSTRATE A VIABLE WAY TO FOLLOW OUR PROPOSED SUGGESTIONS

Sensor nodes are often deployed in harsh environments or unattended locations, which makes it easy for adversaries to break them. Once the adversary compromises a sensor node, she is in a much better position to perform a series of subsequent attacks. Furthermore, the resource-constrained nature of sensor nodes drives designers to improve the performance and unconsciously degrade the security, which makes the situation worse. As such, understanding node capture attacks and exploring the countermeasure is significant to the design of a secure user authentication scheme for WSNs. Accordingly, we proposed some suggestions to node capture attacks in Section 5. In this section, we take Li et al.’s scheme [1] as an example to show a viable way to follow our proposed suggestions. Note that, we keep the original notations of Li et al.’s scheme [1]:

- Unreasonable design intent.
  As our suggested, their scheme does not expose users’ information (such as user identities or unique secret parameters) to sensor nodes, thus their scheme is free from the issue of unreasonable design intent.

- Insecure communication architecture.
  As suggested, the secure model (a) of Fig.5 is chosen. Thus, their scheme is free from the attack Type VIII.

- Inappropriate distribution of SN’s private key.
  As suggested, the private key of sensor node SNj is distributed as h(SNid||w), where w is the long term secret key. Thus, the scheme is resistant to the attack Type II.

- Insecure transmission of some parameters.
  Their user identity, private key of SNj and long term secret key are transmitted securely. As we suggest, user’s identity IDU is transmitted in a form of IDU ⊕ h(D2), where D2 is U’s TUSP_G/U (it is constructed by a public-key technique). Their private key Kgs of SNj is transmitted in a form of Kgs ⊕ rg and h(Kgs||D8||rg||SNid), where rg is TUSP_G/SN. Their long term secret key w is transmitted in a form of h(IDU||w and h(SNid||w). Thus, the scheme is resistant to the attack Type VI and Type IX.

However, their FUSP_G/U (B2) is transmitted with XOR, once the adversary compromises sensor node SNj, then she can eavesdrop transcript M1 which is sent to SNj, and compute DIDu ⊕ D3 ⊕ SNid ⊕ IDu to get FUSP_G/U (B2), then the attack Type III occurs.

As predicted, using FUSP_G/U (B2) in a form of h(FUSP_G/U||TUSP_G/U||*) can settle the issue well, i.e. let D3 = SNid ⊕ h(B2||D2||IDU). Note that D2 is U’s TUSP_G/U. In this way, FUSP_G/U is protected in hash function.

- Inefficient verification of SN or CP
  Li et al.’s scheme follows our suggestion partly: Auth3 of Li et al.’s scheme D3 contains FUSP_G/SN (Kgs) and TUSP_G/SN (rg). Thus their GWN authenticate SNj efficiently; the scheme is secure against attack Type VII.

However, their Auth4 D11 only contains CP_G/SN, which violates our suggestion, thus the adversary can conduct the attack Type X. Note that, from Auth4 of Li et al.’s scheme, we should understand why we suggest Auth4 contains at least CP_G/SN and TUSP_G/U rather than CP_G/SN and FUSP_G/U. To avoid other distractions, we suppose that FUSP_G/U (B2) is securely transmitted, and D11 = h(IDU||D1||D8||B2), then A can get D1 and D8 (i.e. CP_G/SN) with the capability of C1, and carry out an offline dictionary attack with the capability of C2 and C6. Therefore, to achieve users’ verification of CP_G/SN meanwhile not raising such an attack, we recommend to let Auth4 at least contain CP_G/SN and TUSP_G/U.

- Forward secrecy.
  Their scheme follows the principle to achieve forward
Off-line dictionary attack.

Their scheme deploy public-key technology, and let Auth1 \((D_4)\) contain FUSP\(_G\)/\(_U\) \((B_2)\) and TUSP\(_G\)/\(_U\) \((D_2)\). Then with two unknown parameters \((B_2, D_2)\), the adversary cannot conduct off-line dictionary attack. Note that, in Section 4.4, we mention that once the adversary compromises a sensor node, she is in a better position to conduct such an attack via the parameters containing FUSP\(_G\)/\(_U\) \((B_2)\). In Li et al.’s scheme, besides Auth1 \((D_4)\), D3 also contains B2, once the adversary compromises sensor node SN\(_j\), then she can eavesdrop the transcript \(M_3\) that is sent to SN\(_j\), and conduct an off-line dictionary attack using DID\(_u\) \(\oplus\) D3 \(\oplus\) SN\(_{id}\) as verification to test the correctness of guessed password and identity. Thus their scheme is not secure against the attack Type IV. The way to repair this weakness is not difficult and has been mentioned above: let D3 = SN\(_{id}\) \(\oplus\) h(B2 || D2 || D_0). Note that, D2 (TUSP\(_G\)/\(_U\)) is an unknown parameter to the adversary A, thus it can prevent A from constructing D3 with the guessed password and identity to conduct off-line dictionary attack.

The issue of temporary certificate technique.

Their scheme apply the public-key technique to achieve their security and functionality rather than the temporary certificate technique, thus their scheme is free from the issue of temporary certificate technique. Furthermore, combined with the analysis in “unreasonable design intent” and “insecure transmission of some parameters”, their scheme can resist the attack Type V.

From Li et al.’s scheme, we can see that our proposed suggestions are practical and effective. Although the specific methods to achieve our suggestions are various and depend on protocol designers themselves, our suggestions do provide a good reference and guidance for designing a secure multi-factor user authentication schemes for WSNs that is resistant to node capture attacks.

Appendix B: Comparison results in Table 5 on node capture attacks

As shown in Table 5, it is not difficult to find that regardless of whether the user authentication schemes for WSNs provide a formal proof, they are always found having this or that problems, which are caught in a circle of “break-fix-break-fix”. As we mentioned in Section 6, “S6: resistance to node capture attacks” is one of the most popular criterion which cannot be achieve by most of multi-factor user authentication schemes for WSNs. Furthermore, it can be seen that each sub-criterion of S6 is met by more than 10 schemes, meanwhile unmet by at least 10 schemes. This implies the necessity of each of the ten sub-criteria of S6 and the rationality of our taxonomy of node capture attacks.

As shown in Table 5, in the years when node capture attacks were introduced into user authentication protocols, the proposed protocols were difficult to resist most types of node capture attacks. As time go by, the situation of the sub-criteria II and IX have a marked improvement, which indicates that designers have found a good way to securely distribute the private keys of sensor nodes and gateway. This changes is not surprised because the distribution of the private keys are the foundation issue to the security of authentication schemes, it should have been well settled after ten years intensive research. Since the distribution of the private keys of sensor nodes is also a factor causing the attack Type VI, it is not hard to understand why Type VI has the similar situation to Type II. Furthermore, most schemes can resist against the attack Type VII and VIII after 2018. This is because they use the secure communication model (a) of Fig.5 after Wang et al. [3] identified the inherent weaknesses in some of communication models and recommended model (a) for single-gateway settings in 2018.

Also, it can see that node capture attacks have big adverse effect on users: the attack Type III, Type IV and Type V all are popular. The attack Type IV is the outcome of not applying public-key technique or the lack of deep understanding on node capture attacks (so do the attack Type III and Type V). For example, in Jiang et al.’s scheme [4], as we shown in Section 4.4, the adversary with the private key of SN\(_j\) can use the guessed value to compute M8, then conduct the attack, where M8 = h(SK || D_0 || D3 || D_1). The reason why Jiang et al.’s scheme [4] suffers from this attack, is an issue of consciousness rather than technique. Because if they do not assume that the adversary can compromise sensor nodes, they cannot find this attack. Therefore, if we have a well understanding on node capture attacks, this attack can be found and avoid easily. Similarly, if we have realized the adversary has the same capability as a legitimate sensor node, then we will not let the sensor node know user’s identity and transmit important parameters relying on the parameters that can be computed by sensor nodes. In this way, the schemes’ performance on resisting the attack Type IV and V could be better. Accordingly, our comprehensive research on node capture attacks will help to design a scheme that is resistant to the three attacks.

Furthermore, among the ten types of node capture attacks, Type I is the most popular, then Type X and Type V. Type I is essentially an issue of forward secrecy. Since the resource-constrained nature of sensor nodes, it is not easy to design a user authentication scheme for WSNs that provides forward secrecy efficiently. As mentioned in Section 5, it is not difficult to avoid the attack Type X and Type V. However, due to the lack of research on node capture attacks, the adversary’s capabilities are not well understand (i.e. the protocol designers are not very clear about what actually the adversary can do after getting the private key of sensor nodes), thus the protocol designers usually give the sensor node too much authority (such as computing user’s identity) or do not verify CP\(_{SN}\). Under this situation, the attack Type V and Type X become popular.

From Table 5, we can see that the lack of node capture attacks is one of the critical factor resulting in the circle of “break-fix-break-fix”. Naturally, one of the way to break the circle is: proposing a set of comprehensive evaluation criteria, and then exploring the challenges and solutions for achieving each criterion. Evaluation criteria are the cornerstone for the design of protocols. Without a set of complete and reasonable criteria, it is difficult for designers to fully

\[
A = B \times C
\]
consider the security goals of their schemes. If everyone uses their customized criteria to assess their schemes, they may ignore some important security requirements. That will undoubtedly hinder the progress of this area seriously.

However, the lack of understanding on node capture attacks makes this attack related criterion not getting a proper position in the widely-accepted criteria [3]. Before our work, the criterion “resistance to node capture attacks” is included in the criterion “resistance to known attacks”. As such, when designing or analyzing a user authentication scheme for WSNs, this attack naturally is regarded as a normal attack as other simple attacks in the criterion “resistance to known attacks”, thus is overlooked. Furthermore, since the adversary in the criterion “resistance to known attacks” is not allowed to get the victim’s smart card, the attack scenarios where the adversary simultaneous compromises a sensor node $SN_j$ and a user $U_i$’s smart card cannot be captured. These two aspects greatly hinder the design of a secure user authentication for WSNs. Without a proper position in the evaluation criteria, let alone the solution to various security threats. In addition, without effective solution to be followed, designers are also helpless to node capture attacks.

Therefore, our work on node capture attacks not only improves the current evaluation criteria, but also provides a guidance to design a secure user authentication scheme for WSNs that is resistant to node capture attacks. Our larger-scale comparative measurement of 61 representative user authentication schemes for WSNs shows that only two schemes are resistant to node capture attacks, which well indicates the unsatisfactory situation, and also highlights the necessity of our work on node capture attacks.

**REFERENCES**


