Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks

Ding Wang, *Member, IEEE*, Wenting Li, and Ping Wang, *Senior Member, IEEE*

***Abstract*—Dozens of two-factor authentication schemes have been proposed to secure real-time data access in industrial wireless sensor networks (WSNs). However, more often than not, the protocol designers advocate the merits of their scheme, but do not reveal (or unconsciously ignoring) the facets on which their scheme performs poorly. Such lack of an objective, comprehensive measurement leads to the unsatisfactory "break-fix-break-fix" cycle in this research area. In this paper, we make an attempt toward breaking this undesirable cycle by proposing a systematical evaluation framework for schemes to be assessed objectively, revisiting two foremost schemes proposed by Wu *et al.* (2017) and Srinivas *et al.* (2017) to reveal the challenges and difficulties in designing a sound scheme, and conducting a measurement of 44 representative schemes under our evaluation framework, thereby providing the missing evaluation for two-factor schemes in industrial WSNs. This work would help increase awareness of current measurement issues and improve the scientific process in our field.**

***Index Terms*—Evaluation criteria, measurement, password, smart card, and wireless sensor networks (WSNs).**

I. Introduction

NOWADAYS, wireless sensor networks (WSNs) are increasingly becoming an integral part of our daily life and have drawn great attention from both academic communities and industrial worlds. They have been widely used for various critical industrial applications, such as temperature monitoring for precision agriculture [1], power usage monitoring for smart grid [2], and heart beat monitoring for healthcare [3]. Generally, WSNs are built on a set of distributed lightweight sensor nodes, a number of dispersed users, one or more relatively powerful gateway nodes (*GWN*, or so-called base station), which play a key role in the operation of the whole network.

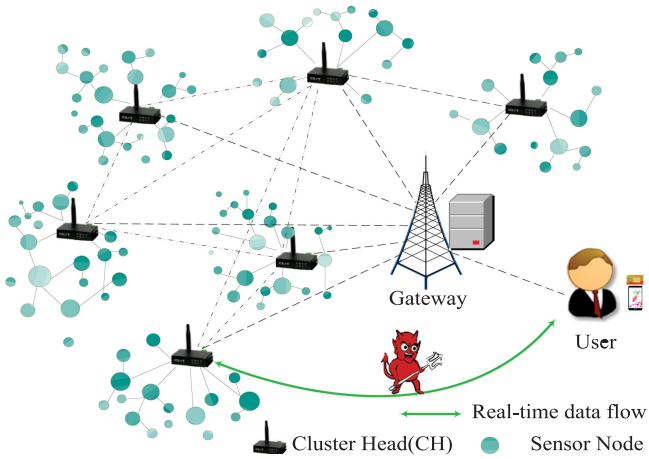

Fig. 1. Real-time application data access in industrial WSNs.

Recently, user's interests in many critical applications have evolved from delay tolerant data communication to real-time data acquisition [4], [5]. To facilitate external users to enjoy the real-time data directly from the target sensor nodes without interacting with the GWNs as demanded, it is important that such sensitive data and user behavior information are well guarded against eavesdropping, intercepting, modification, malicious exploitation, etc. [6]–[8]. Among various security mechanisms, user authentication constitutes the first line of defense as well as the basis of access control: Users shall be first verified by the sensor nodes before being allowed the access to application data. Due to its simplicity, portability, and cryptographic capacity, password authentication using smart cards (so-called two-factor authentication [9]), as shown in Fig. 1, has been widely considered as a promising approach for real-time data acquisition in security critical industrial WSNs.

The past 30 years of research on password-only user authentication schemes has shown that it is incredibly hard to design a single-factor protocol right (see [10]–[12]), and the past 20 years of exploration on two-factor authentication for traditional networks (e.g., the Internet) has proved that it is

Manuscript received August 31, 2017; revised December 25, 2017; accepted April 18, 2018. Date of publication May 8, 2018; date of current version September 4, 2018. This work was supported in part by the National Key Research and Development Plan under Grant 2016YFB0800603 and Grant 2017YFB12 00700, and in part by the National Natural Science Foundation of China under Grant 61472016. Paper no. TII-17-2048. Ding Wang is supported by the "Boya Postdoctoral Fellowship" from Peking University, China. *(Corresponding author: Ping Wang.)*

D. Wang is with the School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China (e-mail: wangdingg@pku.edu.cn).

W. Li is with the School of Software and Microelectronics, Peking University, Beijing 102600, China (e-mail: wentingli@pku.edu.cn).

P. Wang is with the National Engineering Research Center for Software Engineering, School of Software and Microelectronics, Peking University, Beijing 100871, China, and the Key Laboratory of High Confidence Software Technologies (PKU), Ministry of Education, Beijing 100871, China (e-mail: pwang@pku.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2018.2834351

expectedly much harder to make a two-factor protocol right (see [13]–[15]). Besides the challenges in traditional networks, the design of two-factor schemes for WSNs is subjected to two additional challenges. First, sensor nodes are extremely lightweight devices with limited computation capability, storage capacity, and energy resources. Second, WSNs are generally designed for security-critical industrial applications, but often deployed in open/hostile area or left unattended, such as the earth-ocean-atmosphere monitoring system GEOSS [16] and NOPP [17].

Consequently, it is no surprise to see that the past 10 years of research on two-factor authentication for industrial WSNs is full of zig-and-zags, and falls into the unsatisfactory "break-fix-break-fix" cycle (see Fig. 2). In 2009, Das [19] proposed the first smart-card-based password authentication scheme for WSNs, and it opens the new direction for user authentication in WSN environments. Unfortunately, this scheme was pointed out to have serious weaknesses (e.g., no mutual authentication and user anonymity) [20], [21]. Then, Xue *et al.* [22] put forward a temporal-credential-based authentication scheme in 2013 and claimed that their scheme is of robust security. Later, a dozen of improvements (see [23]–[27]) over Xue *et al.*'s scheme have been presented. Among them, Jiang *et al.* [26] showed that Xue *et al.*'s scheme suffers from the privileged insider attack, smart card loss attack, and fails to preserve user anonymity, then they put forward an enhanced version.

Recently, Wu *et al.* [28] analyzed the security of Jiang *et al.*'s scheme [26] and Choi *et al.*'s scheme [29], and pointed out that both schemes are susceptible to offline password guessing attack and user forgery attack. In addition, Jiang *et al.*'s scheme [26] fails to achieve forward secrecy and Choi *et al.*'s scheme [29] lacks user anonymity, and thus they suggested a new scheme [28]. However, in this paper, we demonstrate that Wu *et al.*'s scheme [28] still fails to eliminate the security flaws of smart card loss attack, user impersonation attack, and user anonymity violation attack.

In 2016, to increase scalability, Amin-Biswas [37] proposed a lightweight and comprehensive user authentication and key agreement scheme for multigateway industrial WSNs. However, Srinivas *et al.* [36] revealed that Amin-Biswas's scheme [37] would leak sensors' secret keys and the system key, and it is also vulnerable to server spoofing attack, user impersonation attack, stolen smart card attack, and offline guessing attack. To overcome the identified issues, Srinivas *et al.* [36] further put forward a new scheme. Unfortunately, we find that the scheme in [36] is still subject to various security flaws, such as offline password guessing, user anonymity violation, and node capture attack. Besides reporting security flaws in [28], [36], we also examine the root causes underlying these failures and, accordingly, provide effective countermeasures.

Motivations: In most of these studies, there is no comprehensive criterion available for protocols to be measured objectively, and the protocol designers themselves advocate the merits of their scheme, but do not reveal (or unconsciously overlooking) the aspects on which their scheme performs poorly. Such lack of an objective, comprehensive measurement leads to the unsatisfactory situation: Most of the schemes are found either unable to meet essential security requirements or short of critical properties. In addition, when dealing with the evaluation criteria, little attention has been paid to the underlying system architecture and adversary model. We argue that these three elements are inherently indispensable from each other and should be considered as integral parts. This explains why lots of efforts have been devoted, yet little substantial progress has been made in this research area.

Contributions: In this work, we make an initial step toward breaking this undesirable cycle by proposing a systematical evaluation framework in terms of security, efficiency, and scalability for schemes to be assessed objectively; revisiting two state-of-the-art schemes presented by Wu *et al.* [28] and Srinivas *et al.* [36] to reveal the challenges and difficulties in designing a sound scheme; and conducting a large-scale evaluation of 44 representative schemes under our evaluation framework, thereby providing the missing measurements for two-factor user authentication schemes in industrial WSNs.

Organization: This paper is organized as follows: In Section II, we articulate the system models, adversary model, and evaluation criteria. In Section III, we review Wu *et al.*'s scheme. Section IV describes the weaknesses of Wu *et al.*'s scheme. Section V cryptanalyzes Srinivas *et al.*'s scheme. Our evaluation results of 44 representative schemes are presented in Section VI. Section VII concludes this paper.

II. System Architecture, Adversary Model, and Evaluation Criteria

In this section, we for the first time examine the pros and cons of eight basic system architectures, explicitly define the widely accepted adversary model, and propose a comprehensive yet concrete evaluation criteria set. These three elements are essential in assessing the goodness of a scheme and they together constitute a systematic framework for measuring two-factor authentication schemes for industrial WSNs.

A. System Architecture

Owing to the openness of WSNs, it is challenging to ensure secure and reliable data transmission, monitoring, and timely response of sensitive information. Besides, it becomes imperative to consider the scalability with the increasing applications of WSNs (e.g., military, healthcare, and civilian) in practice [36]. It is natural to see that there is a close relationship among performance, security, and scalability of architecture models in WSNs. Regarding single-gateway WSNs, five basic system models can arise among the user, *GWN*, and sensor node, as concluded by Xue *et al.* [22] in 2013. However, they only deal with single-gateway networks and pay little attention to the multi-gateway environments. In addition, there is no comparison of the goodness among these five models in [22].

With the experience of analyzing more than two hundred two-factor authentication schemes for the client-server architecture and over sixty schemes for WSNs, we provide a summary of eight different types of architecture models that covers both the single-gateway and multigateway environments (see Fig. 3). We show that some of these eight models have their inherent weaknesses. We will test these system models against 44 representative schemes with the usability and security in Table IV.

The first model, i.e., Model (a), is the standard one for single-gateway environments. By using two full rounds of message

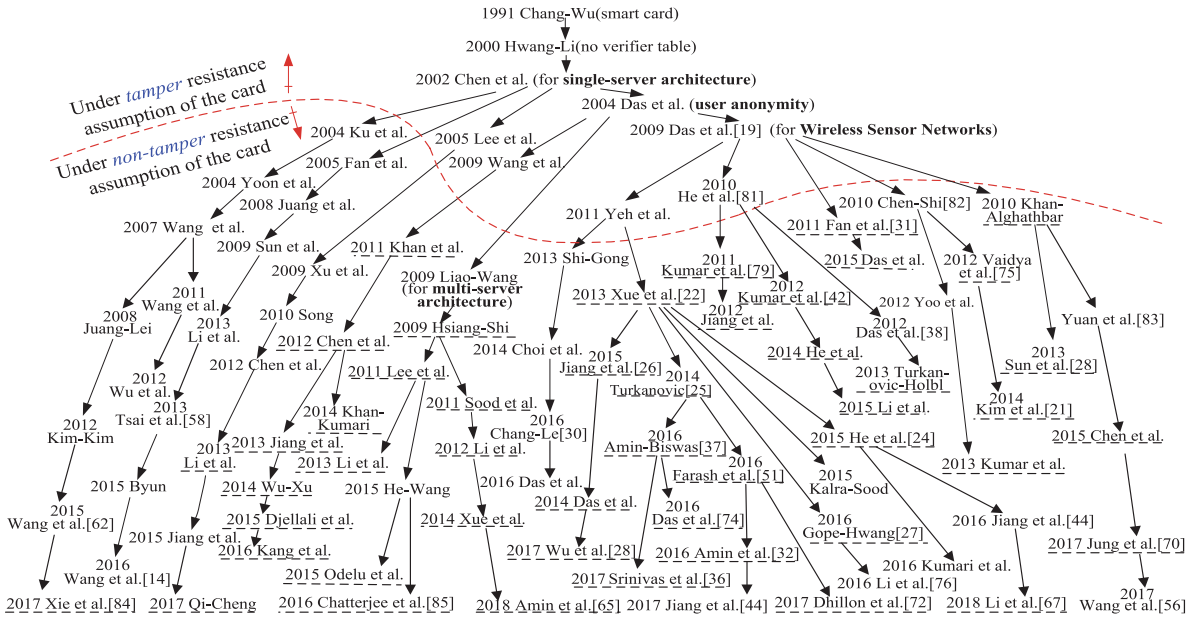

Fig. 2. A brief history of two-factor authentication for industrial WSNs. This figure is based on Fig. 2 of [18]. In most studies, the authors first present attacks on protocol(s) in the parent node, and then give a new scheme and claim it to be better. All schemes underlined cannot attain truly two-factor security.

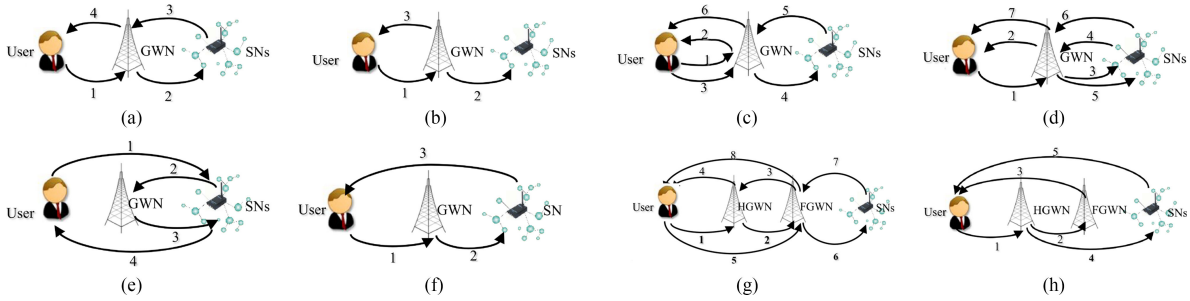

Fig. 3. Eight basic system architectures for user authentication in industrial WSNs. GWN = Gateway node; HGWN = Home GWN; FGWN = Foreign GWN. (a) Typical schemes [27], [30]. (b) Typical schemes [31]. (c) Typical schemes [32]. (d) Typical schemes [33]. (e) Typical schemes [34]. (f) Typical schemes [35]. (g) Typical schemes [36], [37]. (h) Typical schemes [38].

flows, the user, *GWN*, and sensor node can routinely ensure mutual authentication. Note that it can be extended to cater for multigateway networks [e.g., Model (g)]. Generally, once deployed, WSNs are left unattended without big physical changes. However, owing to the limited memory and computation capacity of sensor nodes, there is an increasing need to extend networks with multiple GWNs to increase network capacity, reduce management complexity, and prolong the network lifetime [37]. On the other hand, to eliminate the negative effects of node capture attack and power exhaustiveness of sensor nodes, dynamic node addition has become a very admired attribute in WSNs. Thus, an architecture with scalability (i.e., dynamic node addition) for multigateway environments is very important.

This explains why Model (b) is rarely adopted in recent schemes. More specifically, it is only suitable for user-to-sensor authentication in single-gateway networks, because it requires additional storage overhead to keep user information in *FGWN*. In other words, *FGWN* cannot realize directly communication with users if it does not keep user-specific credentials. This is best illustrated by the Model (h), which is extended from Model (b) and has to keep user-specific credentials. An alternative yet better approach to tackling this problem is to combine Models (a) and (b), i.e., merging Steps 7 and 8 of Model (g).

Model (c) is extended from Model (a) by adding two message flows between the user and GWN. This model is either subject to redundancy or unable to preserve mutual authentication. On the one hand, if the nonce mechanism is employed to ensure freshness of the protocol messages, then the mere two message flows between GWN and the sensor node are inadequate to reach mutual authentication. On the other hand, if the time-stamp mechanism is used to ensure freshness, then only two message flows between the user and GWN are sufficient to achieve mutual authentication. This well explains why many two-factor authentication schemes (e.g., [22], [24], [26]) prefer abandoning Steps 2 and 3 to achieve Model (a).

Model (d) suffers from the same issues with that of Model (c). As for Model (e), it implements mutual authentication with the

help of *GWN*, and is widely employed in early single-gateway WSNs (see [40], [41]). However, after careful analysis, we find that Model (e) is not desirable due to the following two reasons. First, Model (e) allows any user (including the attacker) to communicate with sensor nodes in the first place, and this makes it prone to *GWN* bypassing attack and DoS attack as the computation capacity and memory of sensor nodes are rather limited. It has recently been realized that it is crucial to guarantee that only authorized users are permitted to access sensor nodes in WSN environments (see [26], [39]). Second, Model (e) cannot be extended to multigateway WSN environments, because *FGWN*s are essentially not a managing directory for all sensor nodes of the whole networks, and thus in Step 2 of Model (e), a sensor node is unaware of which *GWN* should it communicate with.

Model (f) is also widely used in earlier schemes (see [19], [38], [42]), yet since *GWN* only forwards messages in Step 2, this model is prone to *GWN* bypassing attack. Moreover, it is intrinsically unable to achieve mutual authentication, because it prevents users from knowing the authenticity of *GWN*, and also prevents *GWN* from knowing the authenticity of sensor nodes. In other words, there is lack of feedback from *GWN* to the user, and thus users are unaware of whether the *GWN* is legitimate or not. Similar issue exists between the sensor node and *GWN*.

The last two models are explicitly designed for multigateway environments. As said earlier, Model (g) can be extended from Model (a) by first seeing *FGWN* as the sensor node and then seeing *FGWN* as the home gateway node (i.e., *HGWN*). In comparison, Model (h) simplifies Model (g) by abandoning three message flows: Steps 3, 6, and 7. What is the role of *FGWN* in Model (g) is beyond comprehension. Typically, *FGWN* is used to handle sensor nodes that roam outside the reach of their *HGWN*, but there is no direct communication flow between *FGWN* and the sensor node in Model (g), and *HGWN* is still used to forward messages to the sensor node. This also indicates that, in Model (g), mutual authentication between *FGWN* and sensor node is intrinsically unattainable.

Summary: We investigate the system models for user authentication in WSNs, and find that some models have inherent weaknesses, and in comparison, we advise to employ Models (a) and (g) to design schemes for single-gateway and multigateway WSNs, respectively. Besides the above-mentioned rather abstract analysis, we further validate our analysis by using two concrete protocols given by Wu *et al.* [28] and Srinivas *et al.* [36] as case studies and by conducting a large-scale evaluation of 44 representative schemes in Section VII.

B. Adversary Model

As the security of a cryptographic scheme can only be assessed under a certain security model, we now explicitly state an adversary model that is consistent with the reality. To our knowledge, this work, following the existing works in [14], [43], [44] while introducing new perspectives, is one of the few ones that explicitly define the capacities of the adversary for user authentication in WSNs. The main capabilities of $\mathcal{A}$ in our model are specified as follows.

C1. The adversary $\mathcal{A}$ is able to offline enumerate all the items in the Cartesian product $\mathcal{D}_{id} \times \mathcal{D}_{pw}$ of identity space $\mathcal{D}_{id}$ and password space $\mathcal{D}_{pw}$ within polynomial time; or able to determine the victim's identity only when assessing the security of a scheme.

C2. The adversary $\mathcal{A}$ is in full control of the exchanged messages between users, sensor nodes, and *GWN*.

C3. The adversary $\mathcal{A}$ may either learn a victim's password or extract sensitive parameters from a victim's smart card, but cannot achieve both.

C4. The adversary $\mathcal{A}$ may obtain the previously agreed session key(s).

C5. The adversary $\mathcal{A}$ may get the *GWN*'s secret key(s) when assessing the eventual failure of the system.

C6. The adversary $\mathcal{A}$ can compromise some sensor nodes.

C7. The adversary $\mathcal{A}$ can create and register as a legitimate user and collude with a legitimate but curious *FGWN* in a multigateway environment.

The capabilities C1∼C4 are in compliance with the standard adversary model for two-factor schemes in generic client-server architecture. More specifically, C1 means that both the password space $\mathcal{D}_{pw}$ and the identity space $\mathcal{D}_{id}$ are quite limited (i.e., $\mathcal{D}_{id} \leq \mathcal{D}_{pw} \approx 10^6$ [45], [46]), and they can be exhaustively enumerated by $\mathcal{A}$ in polynomial time. As user identity is not a secret, it should be regarded as known information when assessing the *security goals* of a protocol [18]. Hence, it shall not build the security of the system on the confidentiality of user identity. The assumption C2 is consistent with the Dolev–Yao model and widely accepted in WSNs [47], while C3 adheres to "the extreme-adversary principle" [14] and captures the essential goal of "truly two-factor security" [48]. The capability C4 captures the situation that previous session key(s) may be acquired by $\mathcal{A}$ due to various reasons like improper erasure and memory leakage (see the "Heartbleed" vulnerability [49]).

Under assumption C5, $\mathcal{A}$ can obtain the *GWN*'s long-time private key(s). This assumption is used only when capturing the property of forward secrecy. The capability C6 is used to model the node capture attack [50], while C7 implies that $\mathcal{A}$ may be a legitimate but curious user. In practice, the capabilities C6 and C7 are realistic because that WSNs are generally deployed in hostile and unattended environments.

C. Evaluation Criteria

We build our evaluation criteria set on the basis of Wang–Wang's criteria set [14], which is originally proposed for the generic client-server architecture. To make it suited for the WSN environments, we perform some adjustifications (tunings) as shown in the fourth column of Table I. Without loss of generality, we take both *GWN* and sensor nodes as the server side, while keeping users as client. It should be noted that the criterion C-4 involves eight different types of traditional and new smart-card-loss attacking scenarios (see [43]) where $\mathcal{A}$ has acquired the victim's smart card, while C-5 copes with scenarios where $\mathcal{A}$ does *not* have the victim's card.

Additionally, we point out that criterion C-5 not only includes the traditional offline password guessing, replay, parallel, de-synchronization, and privileged insider attacks but also involves node capture attack and *GWN* bypassing attack, as well as considering *GWN* impersonation attack and sensor node

TABLE I
A BROAD SET OF 12 INDEPENDENT CRITERIA FOR EVALUATING TWO-FACTOR AUTHENTICATION SCHEMES IN INDUSTRIAL WSNS

Notation	Short term	Detailed meaning for general client/server architecture (see [14])	Adjustifications for WSNs
C-1	No password verifier-table	The server has no need to maintain a verifier-table for keeping the users' passwords or some derived values of the passwords.	Neither of *GWN* nor sensor nodes should keep the passwords related values in the verifier-table.
C-2	Password friendly	The users can freely choose passwords and change it locally.	Remain the same.
C-3	No password exposure	The passwords cannot be obtained or derived by the privileged administrator.	The passwords cannot be obtained or derived by the home/foreign gateways [37].
C-4	No smart card loss attack	The scheme can resist against smart card loss attack, i.e., any adversary or malicious users cannot change the password, recover the password by using offline, online or hybrid guessing attacks from a victim's smart card, or impersonate a victim to login to the system, even if the secret parameters in the card is revealed.	Remain the same.
C-5	Resistance to known attacks	This criteria considers the case in which the attacker is without the victim's smart card, and the scheme can resist various known attacks, including impersonation attack, offline guessing attack, de-synchronization attack, replay attack, parallel attack,key control,stolen verifier-attack, unknown key share attack and known key attack.	The impersonation attack can be divided into user impersonation, *GWN* impersonation and sensor nodes impersonation attacks [24], [37]. The scheme can also resist node capture attack and *GWN* by passing attack [39].
C-6	Sound repairability	The scheme supports smart card revocation, i.e., allowing a user to revoke the smart card but not change his/her identity.	The scheme provides dynamic sensor node addition.
C-7	Provision of key agreement	The client and the server can agree on a session key for subsequent communication during the authentication phase.	Remain the same.
C-8	No clock synchronization	The scheme is not affected by clock synchronization and time-delay, i.e, the server and clients need not to synchronize their time clock with all input devices.	Remain the same.
C-9	Timely typo detection	If a user inputs a wrong password by mistake, she will be timely notified.	Remain the same.
C-10	Mutual authentication	The user and the server can authenticate the identity of each other.	The user, gateway nodes and sensors can authenticate each other [24], [37].
C-11	User anonymity	The scheme provides user identity protection and un-traceability.	User anonymity shall be achieved even if the foreign gateway may collude with legitimate yet malicious users to breach other users' anonymity (see [18]).
C-12	Forward secrecy	The scheme can provide perfect forward secrecy.	Remain the same.

impersonation attack. An admired authentication scheme for WSNs shall guarantee that a captured sensor node will not reveal any sensitive information about other noncompromized sensor nodes or affect previous communications [36], [37]. Furthermore, to preserve mutual authentication between user and server, user and *GWN*, and server and *GWN*, it is essential to ensure that *GWN* is genuinely involved in the protocol operation [24], [51]. In all, a secure scheme for WSNs shall withstand some special attacks such as sensor node capture and gateway bypass.

What needs to be emphasized is that sensor nodes are small devices with scarce energy resources and memory capacity; it is more favorable that we can replace the energy exhausted nodes dynamically [18]. Besides, large-scale WSNs often need to increase their network capacity [52]. Both suggest that the criterion C-6 is necessary when considering node addition in WSNs to achieve sound repairability and scalability.

III. REVIEW OF WU ET AL.'S SCHEME

In 2017, Wu *et al.* [28] proposed an efficient two-factor authentication scheme for the single-gateway environment. Wu *et al.*'s scheme adopts Model (a) as its authentication architecture (see Fig. 3) and has four phases: registration, login, authentication, and password change. To achieve user anonymity, it introduces a session-variant variable a_i along with the user-specific secret parameter $h(ID_G\|x\|a_i)$. During each protocol run, a_i and $h(ID_G\|x\|a_i)$ will be updated to new values and sent to U_i, while *GWN* does not need to keep this value. In this way, Wu *et al.*'s scheme not only achieves user anonymity but also prevents desynchronization attack.

In the following, we briefly review the first three phases of Wu *et al.*'s scheme and some intuitive notations are listed in Table II. At the beginning, *GWN* chooses a point P, which is a generator of the group G over the finite field $E(F_p)$, while G is with an order q.

A. Registration

User Registration: Before accessing the resources of sensor nodes, U_i registers with *GWN* as follows.

1) U_i chooses ID_i, PW_i and a random integer b_i, then computes $HPW_i = h(PW_i\|b_i)$.
2) $U_i \Rightarrow$ *GWN*: $\{ID_i, HPW_i\}$.
3) *GWN* generates a random number a_i and computes $B_1 = h(ID_i\|ID_G\|x) \oplus h(ID_i\|HPW_i\|a_i)$ and $B_2 = h(ID_G\|x\|a_i) \oplus HPW_i$.
4) *GWN* $\Rightarrow U_i$: A smart card with secret parameters $\{B_1, B_2, a_i, P, q\}$.
5) U_i computes $B_3 = h(ID_i\|PW_i) \oplus b_i$ and inserts B_3 into the smart card SC.

Sensor node Registration: For each sensor node S_j, the details are as follows

1) $S_j \Rightarrow$ *GWN*: $\{ID_j\}$.
2) *GWN* computes $B_4 = h(ID_j\|ID_G\|x)$ and sends $\{B_4\}$ to S_j via a secure channel.
3) S_j stores $\{ID_j, B_4\}$.

B. Login and Authentication

This phase realizes mutual authentication and negotiates a session key between U_i and S_j, the details are as follows.

1) U_i inserts his/her smart card and keys ID_i^* and PW_i^*, then the smart card calculates $b_i^* = B_3 \oplus h(ID_i^*\|PW_i^*)$ and $HPW_i^* = h(PW_i^*\|b_i^*)$.
2) SC generates random numbers r_1 and α and computes $C_1 = B_1 \oplus h(ID_i^*\|HPW_i^*\|a_i) \oplus h(ID_i^*\|ID_j\|r_1)$, $C_2 = B_2 \oplus HPW_i^* \oplus r_1$, $C_3 = \alpha \times P$, $C_4 = h(C_1\|C_2\|C_3)$, and $C_5 = E_{r_1}(ID_i^*\|ID_j\|C_1\|C_4)$.
3) $U_i \rightarrow$ *GWN*: $\{C_2, C_3, C_5, a_i\}$.
4) *GWN* computes $r_1 = C_2 \oplus h(ID_G\|x\|a_i)$ and obtains ID_i, ID_j, C_1, and C_4 by decrypting C_5 with r_1.

TABLE II
NOTATIONS AND ABBREVIATIONS

Symbol	Description	Symbol	Description
U_i	ith remote user	x	long-term secret key of *GWN*
S_j	jth sensor node	x_H, x_F	secret key of home gateway *HGWN* and foreign gateway *FGWN*
GWN	gateway node (base station)	p, q	p and p are two larger primes
$\mathcal{A}$	the adversary	SK	session key shared between U_i and S_j
ID_i	identity of user U_i	ID_H, ID_F	identity of home gateway *HGWN* and foreign gateway *FGWN*
PW_i	password of user U_i	$\|$	the string concatenation operation
ID_j	identity of sensor node S_j	$\oplus$	the XOR operation
$\Rightarrow$	a secure channel	$E/D(\cdot)$	symmetric encryption/decryption function
$\rightarrow$	a public channel	$h(\cdot)$	secure collision free one-way hash function

Then, *GWN* verifies whether $C_1 \stackrel{?}{=} h(ID_i\|ID_G\|x) \oplus h(ID_i\|ID_j\|\ r_1)$. If they are not equal, *GWN* aborts.

5) *GWN* computes $B_4 = h(ID_j\|ID_G\|x)$, $C_6 = h(ID_i\|ID_j\|C_3)$, and $C_7 = E_{B_4}(ID_i\|ID_j\|C_6)$.
6) *GWN* $\rightarrow S_j$: $\{C_3, C_7\}$.
7) S_j obtains ID_i, ID_j, and C_6 by decrypting C_7 with B_4. Then, S_j checks the validity of ID_j and $C_6 \stackrel{?}{=} h(ID_i\|ID_j\|C_3)$. If both equals, S_j generates $\beta \in [1, q-1]$ and computes $C_8 = \beta \times P$, $C_9 = \beta \times C_3$, $SK_s = h_1(C_3\|C_8\|C_9)$, $C_{10} = h(ID_j\|ID_i\|SK_s)$, and $C_{11} = h(B_4\|C_8\|C_{10})$.
8) $S_j \rightarrow$ *GWN*: $\{C_8, C_{10}, C_{11}\}$.
9) *GWN* checks whether $C_{11} \stackrel{?}{=} h(B_4\|C_8\|C_{10})$. If they are unequal, *GWN* will terminate; otherwise, *GWN* creates a new nonce a_i^{new} and computes $C_{12} = h(ID_G\|x\|a_i^{\text{new}}) \oplus h(ID_i\|r_1)$, $C_{13} = h(ID_j\|r_1\|a_i) \oplus a_i^{\text{new}}$, and $C_{14} = h(ID_i\|ID_j\|a_i\|a_i^{\text{new}}\|C_3\|C_8\|C_{10}\|C_{12})$.
10) *GWN* $\rightarrow U_i$: $\{C_8, C_{10}, C_{12}, C_{13}, C_{14}\}$.
11) U_i computes $a_i^{\text{new}} = C_{13} \oplus h(ID_j\|r_1\|a_i)$, $C_{15} = \alpha \times C_8$, $SK_u = h_1(C_3\|C_8\|C_{15})$, and checks whether $C_{10} \stackrel{?}{=} h(ID_j\|ID_i\|SK_u)$ and $C_{14} \stackrel{?}{=} h(ID_i\|ID_j\|a_i\|a_i^{\text{new}}\|C_3\|\ C_8\|C_{10}\|C_{12})$. If either does not equal, the session will be aborted. Then, U_i computes $B_1^{\text{new}} = h(ID_i\|HPW_i\|\ a_i) \oplus h(ID_i\|HPW_i\|a_i^{\text{new}})$, $B_2^{\text{new}} = C_{12} \oplus h(ID_i\|r_1) \oplus HPW_i$, and replaces (a_i, B_1, B_2) with $(a_i^{\text{new}}, B_1^{\text{new}}, B_2^{\text{new}})$, separately.

C. Password Change Phase

U_i first needs to interact with *GWN* to authenticate each other, and then change the password. The protocol details are not relevant and omitted.

IV. CRYPTANALYSIS OF WU ET AL.'S SCHEME

Although Wu *et al.*'s scheme [28] is efficient and provides various admirable features, such as password update and perfect forward secrecy, it is still vulnerable to some critical attacks under the realistic adversary model given in Section II-B.

A. Smart Card Loss Attack

The most important goal of a two-factor scheme is to achieve "truly two-factor security" [48]: The compromise of one authentication factor (e.g., the smart card) will not endanger the other authentication factor (i.e., the password). However, Wu *et al.*'s scheme [28] fails to attain this goal.

TABLE III
COMPUTATION TIME OF CRYPTOGRAPHIC OPERATIONS ON COMMON PCS

Experimental platform (common PCs)	Hash T_H (SHA-1)	Sysmm.T_S (AES)	Sysmm. T_S (RC6)	Sysmm. T_S (SMS4)
Pentium IV 3.06 GHz	1.521 μs	0.302 μs	0.096 μs	0.107 μs
Intel i5-2450 2.50GHz	0.623 μs	0.143 μs	0.058 μs	0.064 μs
Intel i7-5500 3.60GHz	0.564 μs	0.076 μs	0.021 μs	0.027 μs

With the capability of C3 (see Section II-B), $\mathcal{A}$ can somehow obtain user's smart card and extract its secret parameters B_2 and B_3 by power analysis [53] and reverse engineering [54]. With the capability of C2, $\mathcal{A}$ can eavesdrop login messages $\{C_2, C_3, C_5, a_i\}$ from the public channel. Further with the capability of C1, $\mathcal{A}$ can *offline* guess U_i's password and identity simultaneously as follows:

Step 1: guesses the value of ID_i^*, PW_i^* from dictionary space $\mathcal{D}_{id}$ and $\mathcal{D}_{pw}$;
Step 2: calculates $b_i^* = B_3 \oplus h(ID_i^*\|PW_i^*)$ and $HPW_i^* = h(PW_i^*\|b_i^*)$, $r_1^* = C_2 \oplus B_2 \oplus HPW_i^*$, where B_2 and B_3 are extracted from U_i's smart card and C_2 are intercepted from the public channel;
Step 3: decrypts $C_5 = E_{r_1^*}(ID_i\|ID_j\|C_1\|C_4)$ using r_1^*;
Step 4: verifies the correctness of (ID_i^*, PW_i^*) by comparing the decrypted ID_i with the guessed ID_i^*; and
Step 5: repeats Steps 1∼4 of the above-mentioned procedure until finds the right value of (ID_i^*, PW_i^*).

The time complexity to conduct the above-mentioned attack is $\mathcal{O}(|\mathcal{D}_{id}| * |\mathcal{D}_{pw}| * (2T_H + T_S))$, where T_H is the running time for Hash operation and T_S is the running time for symmetric encryption/decryption operation. As shown in [45], [46], the sizes of user identity space $|\mathcal{D}_{id}|$ and password space $|\mathcal{D}_{pw}|$ are limited, e,g., $|\mathcal{D}_{pw}| \leq |\mathcal{D}_{id}| \approx 10^6$. Therefore, our attack is practical. To obtain a concrete grasp of the running time of the above-mentioned attack, we utilize the open-source cryptographic library MIRACL to measure the common cryptographic operations on moderate PCs, and the experimental results are listed in Table III. It follows that our above-mentioned attack can be finished within two weeks ($=10^6 \times 10^6 \times (2 \times 0.564\,\mu s + 0.07\mu s)$) when using AES as the symmetric encryption algorithm.

In reality, $\mathcal{A}$ may somehow obtain some side information that are public and related to a specific user, e.g., name, gender, nickname, email, and this enables $\mathcal{A}$ to easily distinguish some passwords (identities) from other ones to be the victim user's name

password (identity). For instance, assume $\mathcal{A}$ obtains U_i's family name "Wang" and birthday "20001010", making it possible to easily eliminate some items like "zhao***" and "***1990" from the dictionary space. Consequently, the actual guessing space of identities and passwords are both far less than 10^6. Furthermore, with the proliferation of cloud computing, $\mathcal{A}$ is able to complete the above-mentioned procedure within a few hours by resorting to Microsoft Azure or Amazon EC2 cloud computing services.

The underlying reason why the above-mentioned attack succeeds is that Wu *et al.*'s scheme violates "the public key principle" [55]: When smart cards are assumed to be nontamper resistant , it is necessary to employ some public key technique to resist offline password guessing attack. Wu *et al.*'s scheme [28] does employ the ECC public key technique, but they only use this technique to achieve forward secrecy of the session keys and *never* use this technique to protect the sensitive authenticator $h(ID_i\|x\|a_i)$. More specifically, $h(ID_i\|x\|a_i)$ is exposed in the formulation of $C_2 = h(ID_i\|x\|a_i) \oplus r_1$, and $\mathcal{A}$ can eliminate the secrecy of $h(ID_i\|x\|a_i)$ and uncover r_1 by computing $r_1 = C_2 \oplus B_2 \oplus HPW_i$. With the help of r_1, $\mathcal{A}$ can decrypt C_5 and perform offline guessing attack.

Accordingly, an effective countermeasure to overcome the above-mentioned pitfall is to first encrypt the random number r_1 with *GWN*'s public key and then XOR the ciphertext with $h(ID_i\|x\|a_i)$ to produce C_2. This approach has been adopted in [14], [56]. Unavoidably, this will incur some additional computation overhead, illustrating the inherent tradeoff between efficiency and security.

B. User Impersonation Attack

Once $\mathcal{A}$ completes the above-mentioned smart card loss attack and obtains the correct ID_i and PW_i, $\mathcal{A}$ can impersonate U_i to login to the system. Considering the following scenario, $\mathcal{A}$ generates new random numbers r_i', α' and computes $C_1' = B_1 \oplus h(ID_i\|HPW_i\|a_i) \oplus h(ID_i\|ID_j\|r_1')$, $C_2' = B_2 \oplus HPW_i \oplus r_1'$, $C_3' = \alpha' \times P$, $C_4' = h(C_1'\|C_2'\|C_3')$, and $C_5' = E_{r_1'}(ID_i\|ID_j\|C_1'\|C_4')$. Then, $\mathcal{A}$ sends a legal message $\{C_2', C_3', C_5', a_i\}$ to *GWN*. After successful authentication by *GWN* (each message is valid), $\mathcal{A}$ receives the response message $\{C_8', C_{10}', C_{12}', C_{13}', C_{14}'\}$ and computes $C_{15}' = \alpha' \times C_8'$, $SK_u = h_1(C_3'\|C_8'\|C_{15}')$ correctly.

The above-mentioned attack procedure builds on the failure of Wu *et al.*'s scheme [28] in achieving "truly two-factor security". With both U_i's smart card and U_i's password, $\mathcal{A}$ is indistinguishable from the real user U_i. Fortunately, there is one way to deal with this problem by integrating a "fuzzy-verifier" [55] with "honeywords" [14]: *GWN* (corresponding to the server S in [14]) can timely detect whether the parameters in U_i's smart card have been extracted or not, and if extracted, *GWN* will suspend the corrupt card and thus block $\mathcal{A}$'s further online guesses. A very recent scheme for WSNs by Wang *et al.* [56] demonstrates the success of "fuzzy-verifier + honeywords".

C. User Anonymity Violation Attack

Many recent schemes (e.g., [27], [57], [58]) that use temporal-credentials to provide user anonymity have been found vulnerable to the desynchronization attack. That is, $\mathcal{A}$ blocks one communication message to break the consistency of states between legitimate parties. The practicality and seriousness of the de-synchronization attack have been intensively discussed in multimedia watermarking protocols (see[59]) and RFID authentication schemes (see [60]), yet it was not until 2014 that Wang *et al.* [61] first paid attention to this type of attack in the research field of *two-factor authentication*.

In 2015, Wang *et al.* [62] revealed that there is no easy way to maintain the consistency of the temporal-credentials between the user and the server. Later on, Wu *et al.* [28] attempted to work out this intractable problem by just keeping the one-time temporal-credentials at user side, with no temporal-credentials at the server side (i.e., *GWN*). Though this alleviates the desynchronization vulnerability, but it makes Wu *et al.*'s scheme [28] unable to achieve user anonymity if $\mathcal{A}$ can return the breach smart card back without detection (which is realistic as introduced in [48]). With the attacking procedure given in Section IV-A, $\mathcal{A}$ can obtain the correct random number r_1, then $\mathcal{A}$ can launch the user anonymity violation attack as follows:

Step 1: intercepts the message $\{C_8, C_{10}, C_{12}, C_{13}, C_{14}\}$ sent from *GWN* to U_i;

Step 2: computes $a_i^{\text{new}} = C_{13} \oplus h(ID_j\|r_1\|a_i)$, where a_i is intercepted from the login message and ID_j is decrypted from C_5, as discussed in Section IV-A; and

Step 3: eavesdrops and tracks U_i's next login request $\{C_2^{\text{new}}, C_3^{\text{new}}, C_5^{\text{new}}, a_i^{\text{new}}\}$ by using a_i^{new}.

Once $\mathcal{A}$ can correlate two distinct sessions from the same user U_i, user activities (e.g., locations, hobbies, and social circle) will be exposed. In a word, Wu *et al.*'s scheme [28] seems well motivated but still fails to achieve user anonymity.

The underlying reason for this failure is that Wu *et al.*'s scheme [28] does not employ some public key technique to preserve user anonymity. This violates the generic principle proved by Wang *et al.* in [18]: Under the nontamper-resistance assumption about the smart cards, public key cryptography is indispensable to attain user anonymity. More specifically, Wu *et al.*'s scheme [28] does employ the ECC public key technique, but they only use this technique to achieve forward secrecy of the session keys and *never* use this technique to protect the session-variant values C_2, C_3, and a_i that is aimed to deliver user anonymity. An effective countermeasure to overcome the above-mentioned pitfall is to first encrypt C_2, C_3, and a_i with *GWN*'s public key and do not send them in plain text.

D. No Timely Password Typo Detection

Another key issue of Wu *et al.*'s scheme is that there is a lack of local password verification mechanism, and the password change phase has to be completed by interacting with *GWN*. As a side effect, this scheme is inherently unable to timely detect the event that U_i has accidentally input an incorrect password. This means that both criteria C-2 and C-9 are not met in Wu *et al.*'s scheme.

An effective countermeasure is to store a fuzzy verifier ($B_0 = h(h(ID_i) \oplus h(PW_i))$ mod n_0) in the card memory, where n_0 is a medium integer: $2^4 \le n_0 \le 2^8$. One can see that there exists $\frac{|\mathcal{D}_{id}|*|\mathcal{D}|}{n_0} \approx 2^{32}$ candidates of (ID, PW) pair to thwart $\mathcal{A}$ when $|\mathcal{D}_{id}| = |\mathcal{D}| = 10^6$ [45] and $n_0 = 2^8$. In the meantime,

GWN keeps a $\mathrm{Honey_L ist}$ that records the bogus secret authenticator $h(ID_i\|x\|a_i) = B_2 \oplus (PW_i^*\|b_i)$, where PW_i^* is a bogus password. In this way, the enhanced scheme can *timely* detect the event that the parameter (i.e., B_2) in U_i's card have been extracted. For more details and rationales of the integration of "fuzzy-verifier + honeywords", readers are referred to [14].

V. Cryptanalysis of Srinivas et al.'s Scheme

In 2017, Srinivas *et al.* [36] demonstrated that Amin *et al.*'s scheme [37] suffers from leakage of sensor secret keys, server impersonation attack, smart card loss attack, etc. To tackle the identified weaknesses, Srinivas *et al.* developed a new scheme with formal proof and claimed that their scheme withstands all the possible known attacks. However, as we will show, Srinivas *et al.*'s scheme is still problematic. It employs Model (g) as its authentication architecture (see Fig. 3) and consists of seven phases. Due to space constraints, we do not describe this scheme, but only show its security weaknesses.

A. Smart Card Loss Attack

In Section IV-A, we have presented a smart card loss attack against Wu *et al.*'s scheme [28]. In this attack, $\mathcal{A}$ needs to breach the user's smart card and also eavesdrop the first protocol flow. This corresponds to the Type-IV smart card loss attack defined in [43]. In the following, we show that Srinivas *et al.*'s scheme [36] is susceptible of two types of smart card loss attack: Type-II and Type-IV. The former type of attack does not need the protocol messages and involves $\mathcal{A}$'s capabilities C1 and C3, while the later need the protocol messages and involves $\mathcal{A}$'s capabilities C1, C2, and C3 (see Section II-B).

Also note that Srinivas *et al.*'s scheme [36] is originally a three-factor one, here we are only interested in its two-factor security by assuming that the third factor (i.e., the biometric) has been known to $\mathcal{A}$. This is realistic as user biometrics are constant during their lives, and how to protect user biometric template is still an open issue [63].

Type-II attack: Suppose U_i's biometric B_i and the secret parameters $\{Y_i, TID_i, C_i, V_i, h(\cdot)\}$ stored in the smart card are somehow obtained by $\mathcal{A}$. At this point, $\mathcal{A}$ can find out U_i's identity and password as follows:

Step 1: guesses U_i's identity ID_i^* and password PW_i^* from dictionary space $\mathcal{D}_{id}$ and $\mathcal{D}_{pw}$;
Step 2: calculates $u^* = C_i \oplus H(B_i)$, $V_i^* = h(ID_i^* \oplus PW_i^* \oplus u^*)$, where C_i is extracted from the smart card;
Step 3: validates the correctness of (ID_i^*, PW_i^*) by comparing the calculated V_i^* with the extracted V_i; and
Step 4: repeats Step 1∼3 until find the correct pair of (ID_i^*, PW_i^*).

The time complexity of this attack is $\mathcal{O}(|\mathcal{D}_{id}| * |\mathcal{D}_{pw}| * T_H + T_B)$ [9], [14]. Generally, it is only needed to calculate the biohashing function once, thus T_B can be ignored in practice. According to the running time in Table III, $\mathcal{A}$ may complete the above-mentioned attacking procedure within 7 days on a Laptop. Furthermore, with the correct identity and password, $\mathcal{A}$ can impersonate U_i as discussed in Section IV-B.

This issue arises due to the inherent "usability-security tension": To achieve local password change (i.e., C-2) and timely typo detection (i.e., C-9), an explicit password verifier $V_i = h(ID_i \oplus PW_i \oplus u)$ is stored in U_i's smart card, yet this verifier leads to a Type-II smart card loss attack.

To eliminate this security issue without loss of usability, a promising countermeasure is to adopt the "fuzzy-verifier" technique [55] and store $V_i{=}h((h(ID_i) \oplus h(u\|PW_i))\ mod\ n)$ in U_i's smart card, where n determines the capacity of (ID, PW) pair, $2^4 \le n \le 2^8$. In this way, even if $\mathcal{A}$ obtains V_i, it can-not determine the correct (ID, PW) from the above-mentioned attack, because there will be $\frac{|\mathcal{D}_{id} * \mathcal{D}_{pw}|}{n} \approx 2^{32}$ candidate (ID, PW) pairs that make $V_i^* = V_i$ in Step 3. To further identify the exactly correct (ID, PW) pair, $\mathcal{A}$ needs to interact with *GWN*, and we can adopt the "honeywords" technique [14] to confine $\mathcal{A}$'s advantage to a very limited value.

Type-IV attack: In the above-mentioned attack, $\mathcal{A}$ does not need the protocol messages. This attack needs the protocol messages, and involves $\mathcal{A}$'s capabilities C1, C2, and C3. With C3 (see Section II-B), $\mathcal{A}$ can somehow obtain user's smart card and extract its secret parameters $\{Y_i, TID_i, C_i, V_i, h(\cdot)\}$. With C2, $\mathcal{A}$ can eavesdrop the login messages $\{TID_i, ID_{SN_j}, D_1, D_2, T_1\}$ from the public channel. Further with C1, $\mathcal{A}$ can *offline* guess U_i's password and identity simultaneously as follows:

Step 1: picks a pair (ID_i^*, PW_i^*) from dictionary space $\mathcal{D}_{id}$ and $\mathcal{D}_{pw}$;
Step 2: computes $K_i^* = Y_i \oplus h(PW_i^*\|u\|ID_i^*)$, where $u = C_i \oplus H(B_i)$ and B_i is U_i's biometric;
Step 3: computes $DID_i^* = h(ID_i^*\|u)$;
Step 4: computes $r_i^* = D_1 \oplus h(K_i^*\|DID_i^*\|ID_{SN_j})$;
Step 5: computes $D_2^* = h(DID_i^*\|r_i^*\|TID_i\|K_i^*\|T_1\|ID_{SN_j})$;
Step 6: validates the correctness of (ID_i^*, PW_i^*) by checking if D_2^* equals the intercepted D_2; and
Step 7: repeats Step 1∼6 of the above-mentioned procedure until find the correct pair of (ID_i^*, PW_i^*).

The time complexity of this attack is $\mathcal{O}(|\mathcal{D}_{id}| * |\mathcal{D}_{pw}| * (4T_H + T_B))$, and $\mathcal{A}$ may complete the procedure within 28 days on a Laptop. In comparison, the Type-II smart card loss attack is more practical.

B. No User Untraceability

User untraceability is the advanced property of user anonymity. With this property achieved, there will be no leakage of user-specific information that lead $\mathcal{A}$ to track users' activities, login history, etc. In [36], Srinivas *et al.* claimed that "the use of pseudo identity provides anonymity"; however, this is not true. In their scheme, U_i's pseudo-identity TID_i is constant in all login sessions and unique for U_i. Thus, TID_i can be regarded as U_i's identity, which can be abused by $\mathcal{A}$ to track U_i. Therefore, Srinivas *et al.*'s scheme fails to attain user untraceability. One possible countermeasure is to employ some public-key technique to conceal the user-specific, static information within the session-variant values like that of [14].

C. Node Capture Attack

Usually, WSNs are placed in hostile and unattended environments and commonly carry out extremely sensitive missions (e.g., military and healthcare monitoring). Thus, sensor nodes are rich targets. Srinivas *et al.* explicitly assumed that "the adversary can readily compromise all the secret information of the captured sensor nodes" and claimed that an attacker against their scheme "cannot derive three critical parameters r_i, r_j, r_h at a time from the communication messages."

However, we find Srinivas *et al.*'s scheme cannot fulfill their claim. Once $\mathcal{A}$ captures the sensor node S_j, it can compute the session key of any previous protocol run (say mth run):

Step 1: intercepts the message $\{TID_i, D_3, D_4, D_5, D_6, T_2\}$ that *HGWN* sends to S_j, as well as $\{D_7, D_8, T_3\}$ that S_j sends to *HGWN*, in the mth protocol run;

Step 2: extracts the secret parameter P_j and the registration time T_r from S_j's memory, which is realistic since S_j is not equipped with tamper resistant hardware;

Step 3: computes $r_h = h(P_j \| T_2 \| T_r \| ID_j \| TID_i) \oplus D_3$, $r_i = h(P_j \| TID_i \| r_h \| T_2) \oplus D_4$, and $DID_i = h(P_j \| r_i \| r_h \| T_2) \oplus D_5$;

Step 4: computes $r_j = h(P_j \| r_h \| T_3)$; and

Step 5: computes the mth session key $SK_m = h(DID_i \| r_i \| r_j \| r_h \| ID_j)$.

The above-mentioned attacking procedure shows that $\mathcal{A}$ can derive the "critical parameters r_i, r_j, and r_h at a time from the communication messages," invalidating Srinivas *et al.*'s claim. Once a sensor node is compromised, all its previous communications will be breached. This problem arises because this scheme violates the forward secrecy principle [55]. This principle states that public-key technique is indispensable to achieve forward secrecy and at least two exponential operations are required to be carried out at the server-side. This principle is generic and applicable for WSNs. Accordingly, we can resort to the ElGamal cryptosystem (see Xie *et al.*'s scheme for a concrete example [84]) or the Chebyshev chaotic maps (see Chatterjee *et al.*'s for a concrete example [85]).

VI. A Comparative Assessment of Existing Two-factor Schemes for Industrial WSNs

To illustrate the effectiveness of our evaluation framework, we provide a comparative assessment of 44 representative two-factor schemes for WSNs by evaluating whether the 12 criteria in Table I have been reached under the security model stated in Section II-B. The results are summarized in Table IV. To ensure accuracy and validity of our results, we first conduct the evaluation independently by each author, and a few disagreements arise. Then, we focus on the disagreements and settle them through face to face discussion. This guarantees that our evaluation results are highly reproducible.

Among the 44 schemes evaluated, seven were constructed before 2011 where smart cards are generally assumed to be tamper-resistant. Unsurprisingly, these early four schemes attain poor security under our new security model (see the bottom of Table IV), while more recent schemes (e.g., [44], [56], [66]) generally perform much better. Under our evaluation framework, there is a trend as follows: More recent the scheme is, more satisfactory the scheme will be. This is sensible, for research progresses as time goes on.

Nevertheless, this trend would not be evident had these 44 schemes been measured by previous evaluation frameworks (i.e., [14], [86]–[88]). More specifically, the criteria set in [86] primarily comprises of our criteria C-2∼C-5, and thus the differences between the schemes proposed in 2010 (see [81]–[83]) and the schemes in 2017 (see [44], [56], [66]) cannot be distinguished; the criteria set in [87] considers "protocol efficiency" and, most critically, no adversary model is explicitly specified in [87], all this makes it vague and hardly workable to assess a scheme; the criteria set in [88] takes no consideration of the important "usability-security tension" (see Section V-A), for it overlooks the desirable property "freely password change" (i.e., C-2); employing the criteria set in [14] cannot uncover the special security threats arising in WSNs (such as the node capture attack in Section V-C and the GWN collusion attack in [18]).

Generally, as time goes on, schemes are becoming more desirable in terms of both security and scalability, yet efficiency is an exception. A plausible reason is that a recent work by Wang–Wang [18] proves that if smart cards are assumed to be nontamper resistant, public-key cryptographic primitives will be indispensable for achieving user anonymity (untraceability). Thus, recent schemes tend to employ public-key techniques. Another trend is that, as time goes on, more and more schemes are analyzed with a formal method (e.g., complexity-based provable security, symbol-based logic, and/or automated formal verification tools). Though a formal proof is no silver bullet for ensuring real-world security, schemes do generally perform better when armed with a formal proof. All in all, both trends uncovered by our framework partially corroborate the soundness of our evaluation framework.

Table IV also shows that Model (a) (e.g.,[19], [23], [37]), Model (e) (e.g., [51], [78], [80]), and Model (f) [24] are the most commonly used models for single-gateway WSNs due to its simplicity, while Model (g) is the preferred option for multi-gateway WSNs (e.g., [36], [37]). Accordingly, we advise to follow Model (a) when designing a scheme for single-gateway WSNs due to its simplicity, and to follow Model (g) for multi-gateway WSNs due to its robustness and scalability.

In a microcosmic point of view, we can find that each criterion is *met* by no less than five schemes and *unsatisfied* by no less than three schemes. *This indicates that each of the 12 criteria is necessary.* What is more, no scheme can accomplish all our 12 criteria—the only scheme that can fulfill 11 criteria is given by Wang *et al.* in 2017 [56] and the only scheme achieving 10 criteria is given by Jiang *et al.* in 2017 [44]. *This implies that our criteria set is comprehensive.* This also outlines the urgent needs for more research forces to design an ideal scheme that satisfies all the 12 criteria. After a careful investigation, one can find that both Wang *et al.*'s [56] and Jiang *et al.*'s [44] schemes adopt the "fuzzy-verifier" technique to achieve the criteria C-2, C-4, and C-9 simultaneously (see Section IV-D). Many schemes achieve fewer criteria because they suffer from the same "usability-security tension" as shown in Section V-A: The criterion C-2 (or C-9) and C-4 cannot be satisfied simultaneously. *This indicates that separating C-4 from C-5 is necessary*, which is opposite to the framework in [86].

TABLE IV
MEASURING SECURITY, USABILITY, AND SCALABILITY OF 44 TWO-FACTOR AUTHENTICATION SCHEMES FOR INDUSTRIAL WSNS

Protocol		Reference	Evaluation criteria: C-1: *No password verifier table*	C-2: *Password Friendly*	C-3: *No Password exposure*	C-4: *No smart card loss attack*	C-5: *Resistance to known attacks*	C-6: *Sound repairability*	C-7:*Provision of key agreement*	C-8: *No clock synchronization*	C-9: *Timely typo detection*	C-10: *Mutual authentication*	C-11:*User anonymity*	C-12: *Forward secrecy*	System model	Formal methods: Complexity-based provable security	Symbol-based logic	Automated formal verification tools	Protocol Efficiency: User computational cost	*GWN* computational cost	Sensor computational cost
Wazid et al.	2018	[64]	✓	✓	✓	·	·	✓	✓	·	✓	✓	·	·	Model (a)	✓	·	✓	$T_B + 13T_H + 2T_S$	$5T_H + 4T_S$	$4T_H + 2T_S$
Amin et al.	2018	[65]	✓	✓	✓	·	·	·	✓	·	✓	✓	✓	·	Model (a)	·	✓	✓	$12T_H$	$16T_H$	$6T_H$
Ali et al.	2018	[66]	✓	✓	✓	·	·	✓	✓	·	✓	✓	·	·	Model (a)	·	✓	✓	$2T_S + 6T_H$	$5T_S + 13T_H$	$T_S + 5T_H$
Li et al.	2018	[67]	✓	✓	✓	·	✓	·	✓	✓	✓	✓	·	·	Model (f)	·	✓	·	$2T_E + 8T_H$	$T_E + 9T_H$	$4T_H$
Wu et al.	2018	[68]	✓	·	✓	✓	·	·	✓	✓	·	✓	·	·	Model (a)	·	·	✓	$11T_H$	$17T_H$	$6T_H$
Wu et al.	2017	[69]	✓	·	✓	✓	·	·	✓	·	·	·	✓	·	Model (a)	·	·	✓	$9T_H$	$11T_H$	$4T_H$
Srinivas et al.	2017	[36]	✓	✓	✓	·	·	✓	✓	·	✓	✓	·	·	Model (g)	·	✓	✓	$10T_H$	$13T_H$	$6T_H$
Wu et al.	2017	[28]	✓	·	✓	·	✓	·	✓	✓	·	✓	·	✓	Model (a)	✓	·	·	$2T_E + T_S + 11T_H$	$2T_S + 11T_H$	$2T_E + T_S + 4T_H$
Wang et al.	2017	[56]	✓	✓	✓	✓	✓	·	✓	✓	✓	✓	✓	✓	Model (a)	·	✓	·	$10T_H + 3T_E + T_B$	$11T_H + T_E$	$4T_H + 2T_E$
Jiang et al.	2017	[44]	✓	✓	✓	✓	✓	✓	✓	·	✓	✓	✓	·	Model (a)	·	·	✓	$T_P + 8T_H$	$T_P + 12T_H$	$5T_H$
Jung et al.	2017	[70]	✓	✓	✓	·	·	·	✓	·	✓	✓	·	·	Model (a)	✓	✓	·	$11T_H$	$11T_H$	$4T_H$
Das et al.	2017	[52]	✓	✓	✓	✓	✓	·	✓	·	✓	✓	·	✓	Model (a)	·	·	✓	$12T_H$	$15T_H$	$5T_H$
Xiong et al.	2017	[71]	✓	✓	✓	·	·	·	✓	·	✓	·	·	·	Model (a)	·	✓	·	$9T_H + 2T_S$	$11T_H + 2T_S$	$4T_H$
Dhillon et al.	2017	[72]	✓	✓	✓	·	·	·	✓	·	✓	✓	·	·	Model (a)	·	·	✓	$8T_H$	$8T_H$	$6T_H$
Lu et al.	2016	[73]	✓	✓	✓	·	·	·	✓	·	✓	✓	✓	✓	Model (a)	·	✓	✓	$7T_H + 2T_S$	$5T_H + 3T_S$	$4T_H + 2T_S$
Das et al.	2016	[74]	✓	✓	✓	·	✓	✓	✓	·	✓	✓	·	✓	Model (e)	✓	✓	✓	$2T_E + 12T_H$	$10T_H$	$2T_E + 9T_H$
Amin et al.	2016	[32]	✓	✓	✓	·	·	✓	✓	✓	✓	✓	·	·	Model (c)	·	✓	✓	$12T_H$	$15T_H$	$5T_H$
Amin-Biswas	2016	[37]	✓	✓	✓	·	·	✓	✓	·	✓	✓	·	·	Model (g)	·	✓	✓	$7T_H$	$8T_H$	$5T_H$
Gope-Hwuang	2016	[27]	✓	✓	✓	·	·	·	✓	·	✓	✓	✓	·	Model (a)	·	·	·	$7T_H$	$9T_H$	$3T_H$
Farash et al.	2016	[51]	✓	✓	✓	·	·	·	✓	·	✓	✓	·	·	Model (e)	·	✓	✓	$11T_H$	$14T_H$	$7T_H$
Vaidya et al.	2016	[75]	✓	✓	·	·	·	·	✓	·	✓	✓	·	·	Model (a)	·	✓	·	$8T_H$	$6T_H$	$3T_H$
Chang-Le	2016	[30]	✓	✓	✓	·	·	·	✓	·	·	·	·	·	Model (a)	✓	·	·	$7T_H$	$8T_H$	$5T_H$
Li et al.	2016	[76]	✓	✓	✓	·	·	✓	✓	✓	✓	✓	·	✓	Model (a)	·	·	·	$3T_P + 5T_H$	$T_P + 6T_H$	$2T_P + 4T_H$
He et al.	2015	[24]	✓	·	✓	·	·	·	✓	·	·	✓	✓	·	Model (f)	·	✓	·	$6T_H$	$10T_H$	$7T_H$
Jiang et al.	2015	[26]	✓	✓	·	·	·	·	✓	·	·	✓	✓	·	Model (f)	·	·	·	$7T_H$	$10T_H$	$5T_H$
Turkanovic et al.	2014	[25]	✓	✓	✓	·	·	·	✓	·	✓	✓	·	·	Model (e)	·	·	·	$7T_H$	$7T_H$	$5T_H$
Kim et al.	2014	[21]	✓	✓	·	·	·	·	✓	·	✓	✓	·	·	Model (a)	·	·	·	$8T_H$	$8T_H$	$2T_H$
Xue et al.	2013	[22]	·	✓	✓	·	·	·	✓	·	✓	✓	·	·	Model (f)	·	·	·	$7T_H$	$13T_H$	$6T_H$
Sun et al.	2013	[33]	✓	✓	✓	·	·	·	·	✓	·	✓	·	·	Model (d)	·	·	·	$2T_H$	$5T_H$	$2T_H$
Althobaiti et al.	2013	[77]	·	✓	✓	·	·	·	✓	·	✓	✓	·	·	Model (f)	·	·	·	$4T_H$	$T_H + T_M$	$3T_H + T_M + 4T_S$
Li et al.	2013	[23]	✓	✓	✓	·	·	✓	✓	·	✓	✓	✓	✓	Model (f)	·	·	·	$9T_H$	$11T_H$	$6T_H$
Kumar et al.	2012	[42]	✓	·	✓	·	·	·	·	✓	·	✓	✓	·	Model (f)	·	·	·	$4T_H + 2T_S$	$1T_H + 3T_S$	$1T_H + 2T_S$
Hsiao et al.	2012	[78]	✓	·	✓	·	·	·	·	·	·	·	·	·	Model (e)	·	·	·	$4T_H$	$5T_H$	$3T_H$
Das et al.	2012	[38]	✓	✓	✓	·	·	·	✓	·	✓	·	·	·	Model (h)	·	·	·	$5T_H + 1T_S$	$3T_H + T_S$	$2T_H + T_S$
Kumar et al.	2011	[79]	✓	✓	✓	·	·	·	·	·	✓	✓	·	·	Model (e)	·	·	✓	$4T_H + 2T_S$	$4T_H + 2T_S + T_M$	$T_H + 2T_S + T_M$
Fan et al.	2011	[31]	✓	✓	·	·	·	·	✓	·	✓	·	·	·	Model (b)	·	·	·	$6T_H$	$6T_H$	$2T_H$
Yeh et al.	2011	[80]	✓	✓	✓	·	·	·	✓	·	✓	·	·	✓	Model (e)	·	·	·	$T_H + 2T_P$	$4T_H + 4T_P$	$3T_H + 2T_P$
He et al.	2010	[81]	✓	✓	✓	·	·	·	·	·	✓	·	·	·	Model (f)	·	·	·	$5T_H$	$5T_H$	T_H
Chen et al.	2010	[82]	✓	·	·	·	·	·	·	·	·	·	·	·	Model (f)	·	·	·	$4T_H$	$5T_H$	$2T_H$
Yuan et al.	2010	[83]	✓	✓	·	·	·	·	·	·	✓	·	✓	·	Model (f)	·	·	·	$4T_H$	$4T_H$	T_H
Vaidya et al.	2010	[20]	✓	✓	·	·	·	·	·	·	✓	·	✓	·	Model (a)	·	·	·	$6T_H$	$4T_H$	$2T_H$
Das	2009	[19]	✓	·	·	·	·	·	·	·	·	·	✓	·	Model (f)	·	·	·	$4T_H$	$4T_H$	T_H
Tseng et al.	2007	[41]	✓	·	·	-	·	·	·	·	-	·	·	·	Model (e)	·	·	·	T_H	$3T_H$	T_H
Wong et al.	2006	[40]	·	·	·	-	·	·	·	·	-	·	·	·	Model (e)	·	·	·	-	$3T_H$	T_H

†When confronting a three-factor scheme, we assume that the biometric factor has been known to $\mathcal{A}$, resulting in a two-factor scheme that can be assessed with our evaluation framework in Sec. II. Note that ✓ means achieving the corresponding goal, while · not; T_H: operation time for one-time hash; T_E: operation time for public key encryption and decryption operation; T_P: operation time for elliptic curve point multiplication; T_S: operation time for symmetric encryption and decryption; T_B: operation time for fuzzy extracting biometric info; T_M: operation time for a MAC function.

We emphasize that, in choosing a particular two-factor scheme to be included into the evaluation Table IV, we do not necessarily endorse that it is superior to alternatives not appearing in the table—only due to that it is of high representativeness, or that it somehow illuminates which line of research (from a point view of the development history tree, see Fig. 2) it lies and what goals this line of research can attain. Here we mainly focus on schemes for WSNs because different application environments/architectures may be faced with quite varied security threats and functional requirements, and thus fair comparison is virtually impossible under a single adversary model.

VII. CONCLUSION

In this work, we have made a substantial step toward breaking the vicious "break-fix-break-fix" cycle in the two-factor authentication research domain for industrial WSNs. To this aim, we first investigate the pros and cons of eight basic system architectures, explicitly define the widely accepted adversary model, and propose a comprehensive criteria set of twelve independent evaluation metrics. Then, we have cryptanalyzed two foremost schemes presented by Wu *et al.* and Srinivas *et al.* to reveal the challenges and difficulties in designing a sound scheme. Finally, we have conducted an extensive evaluation of 44 representative two-factor schemes under our evaluation framework, thereby providing the missing measurements for two-factor authentication schemes in industrial WSNs. Our evaluation results show that all existing schemes are not ideal, calling for more principled research on this area.

REFERENCES

[1] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and secured medical data transmission and analysis for wireless sensing healthcare system," *IEEE Trans. Ind. Informat.*, vol. 13, no. 3, pp. 1227–1237, Jun. 2017.

[2] R. Tan, D. E. Phillips, M.-M. Moazzami, G. Xing, and J. Chen, "Unsupervised residential power usage monitoring using a wireless sensor network," *ACM Trans. Sensor Netw.*, vol. 13, no. 3, 2017, Art no. 20.

[3] C. Habib, A. Makhoul, R. Darazi, and C. Salim, "Self-adaptive data collection and fusion for health monitoring based on body sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 6, pp. 2342–2352, Dec. 2016.

[4] X. Ding, Y. Tian, and Y. Yu, "A real-time big data gathering algorithm based on indoor wireless sensor networks for risk analysis of industrial

operations," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1232–1242, Jun. 2016.
[5] C. Lu *et al.*, "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1013–1024. May 2016.
[6] P. Zeng, K.-K. R. Choo, and D.-Z. Sun, "On the security of an enhanced novel access control protocol for wireless sensor networks," *IEEE Trans. Consum. Electron.*, vol. 56, no. 2, pp. 566-569, May 2010.
[7] K.-K. R. Choo, L. Rokach, and C. Bettini, "Mobile security and privacy: Advances, challenges, and future research directions," *Pervasive Mobile Comput.*, vol. 32, pp. 1–2, 2016.
[8] L. Wu, B. Chen, K.-K. R. Choo, and D. He, "Efficient and secure searchable encryption protocol for cloud-based internet of things," *J. Parallel Distrib. Comput.*, vol. 111, pp. 152–161, 2018.
[9] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Depend. Sec. Comput.*, vol. 12, no. 4, pp. 428–442, Jul./Aug. 2015.
[10] S. Shin and K. Kobara, "Security analysis of password-authenticated key retrieval," *IEEE Trans. Depend. Sec. Comput.*, vol. 14, no. 5, pp. 573–576, Sep./Oct. 2017.
[11] Z. Zhao, Z. Dong, and Y. G. Wang, "Security analysis of a password-based authentication protocol proposed to IEEE 1363," *Theoretical Comput. Sci.*, vol. 352, no. 1, pp. 280–287, 2006.
[12] R. W. Lai, C. Egger, D. Schroder, and S. S. Chow, "Phoenix: Rebirth of a cryptographic password-hardening service," in *Proc. 26th USENIX Security Symp., 2017*, pp. 899–916.
[13] X. Huang, X. Chen, J. Li, and Y. Xiang, L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1767–1775, Jul. 2014.
[14] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Trans. Depend. Sec. Comput.*, to be published.
[15] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Netw.*, vol. 27, pp. 159–194, 2015.
[16] "Taking the pulse of the planet: Epa's remote sensing information gateway," Office of the Science Advisor. 2014. [Online]. Available: http://www.epa.gov/geoss
[17] "The National Oceanographic Partnership Program (NOPP)," 2017. [Online]. Available: http://www.nopp.org/
[18] D. Wang and P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions," *Comput. Netw.*, vol. 73, pp. 41–57, 2014.
[19] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.
[20] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in *Proc. IEEE 6th Int. Conf. Wireless Mobile Comp. Netw. Commun., 2010*, pp. 600–606.
[21] J. Kim, D. Lee, W. Jeon, Y. Lee, and D. Won, "Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks," *Sensors J.*, vol. 14, no. 4, pp. 6443–6462, 2014.
[22] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 316–323, 2013.
[23] C.-T. Li, C.-Y. Weng, and C.-C. Lee, "An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks," *Sensors J.*, vol. 13, no. 8, pp. 9589–9603, 2013.
[24] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Inf. Sci.*, vol. 321, pp. 263–277, 2015.
[25] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, 2014.
[26] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 6, pp. 1070–1081, 2015.
[27] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7124–7132, Nov. 2016.
[28] F. Wu, L. Xu, S. Kumari, and X. Li, "A new and secure authentication scheme for wireless sensor networks with formal proof," *Peer-to- Peer Netw. Appl.*, vol. 10, no. 1, pp. 16–30, 2017.
[29] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors J.*, vol. 14, no. 6, pp. 10 081–10 106, 2014.
[30] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.
[31] R. Fan, D. He, X. Pan, and L. Ping, "An efficient and dos-resistant user authentication scheme for two-tiered wireless sensor networks," *J. Zhejinag Univ. Sci. C*, vol. 12, no. 7, pp. 550–560, 2011.
[32] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Comput. Netw.*, vol. 101, pp. 42–62, 2016.
[33] D. Sun, J. Li, Z. Feng, Z. Cao, and G. Xu, "On the security and improvement of a two-factor user authentication scheme in wireless sensor networks," *Pers. Ubiquitous Comput.*, vol. 17, no. 5, pp. 895–905, 2013.
[34] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 316–323, 2013.
[35] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ecc for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, 2016.
[36] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Netw.*, vol. 54, pp. 147–169, 2017.
[37] R. Amin and G. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Netw.*, vol. 36, pp. 58–80, 2016.
[38] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 35, no. 52, pp. 1646–1656, 2012.
[39] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Netw.*, vol. 20, pp. 1–15, 2014.
[40] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Sensor Netw. Ubiquitous Trustworthy Comput., 2006*, vol. 1, Art no. 1636182.
[41] H.-R. Tseng, R.-H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Global Telecommun. Conf., 2007*, pp. 986–990.
[42] P. Kumar, S.-G. Lee, and H.-J. Lee, "E-sap: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012.
[43] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The request for better measurement: A comparative evaluation of two-factor authentication schemes," in *Proc. 11th ACM ASIA Conf. Commun. Security, 2016*, pp. 475–486.
[44] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.
[45] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, "Targeted online password guessing: An underestimated threat," in *Proc. SIGSASC Conf. Comput. Commun. Security, 2016*, pp. 1242–1254.
[46] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.
[47] Z. Benenson, E.-O. Blaß, and F. C. Freiling, "Attacker models for wireless sensor networks," *Inf. Technol. Method*, vol. 52, no. 6, pp. 320–324, 2010.
[48] D. Wang and P. Wang, "Offline dictionary attack on password authentication schemes using smart cards," in *Proc. Inf. Security, 2013*, pp. 221–237.
[49] "Heartbleed – openssl zero-day bug leaves millions of websites vulnerable," Apr. 2014. [Online]. Available: http://www.tuicool.com/articles/yyUfUz
[50] P. Tague and R. Poovendran, "Modeling node capture attacks in wireless sensor networks," in *Proc. IEEE 46th Annu. Allerton Conf. Commun. Control Comput.*, 2008, pp. 1221–1224.
[51] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, 2016.
[52] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *Int. J. Commun. Syst.*, vol. 30, no. 1, 2017, Art no. e2933.
[53] N. Veyrat-Charvillon and F.-X. Standaert, "Generic side-channel distinguishers: Improvements and limitations," in *Proc. Annu. Cryptology Conf., 2011*, pp. 354–372.

[54] K. Nohl, D. Evans, S. Starbug, and H. Plötz, "Reverse-engineering a cryptographic RFID tag." in *Proc. USENIX Security Symp., 2008*, vol. 28.
[55] C.-G. Ma, D. Wang, and S.-D. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," *Int. J. Commun. Syst.*, vol. 27, no. 10, pp. 2215–2227, 2014.
[56] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sens.*, vol. 17, no. 12, 2017, Art no. 2946.
[57] F. Wen, "A more secure anonymous user authentication scheme for the integrated epr information system," *J. Med. Syst.*, vol. 38, no. 5, p. 42, 2014.
[58] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Novel anonymous authentication scheme using smart cards," *IEEE Trans. Ind. Inf.*, vol. 9, no. 4, pp. 2004–2013, Nov. 2013.
[59] P. R. Alface and B. B. Macq, "Feature-based watermarking of 3d objects: Toward robustness against remeshing and desynchronization," *Proc. SPIE*, vol. 5681, pp. 400–408, 2005.
[60] M. H. Yang, "Across-authority lightweight ownership transfer protocol," *Electron. Comm. Res. Appl.*, vol. 10, no. 4, pp. 375–383, 2011.
[61] D. Wang and P. Wang, "On the usability of two-factor authentication," in *Proc. 10th Int. Conf. Security Privacy Commun. Netw., 2014*, pp. 141–150.
[62] D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity," *Inf. Sci.*, vol. 321, pp. 162–178, 2015.
[63] N. Memon, "How biometric authentication poses new challenges to our security and privacy [in the spotlight]," *IEEE Signal Process. Mag.*, vol. 34, no. 4, pp. 196–194, Jul. 2017.
[64] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," *Sensors*, vol. 17, no. 3, p. 644, 2017.
[65] R. Ali, A. K. Pal, S. Kumari, M. Karuppiah, and M. Conti, "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring," *Future Generation Comput. Syst.*, vol. 84, pp. 200–215, 2018.
[66] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, 2018.
[67] F. Wu *et al.*, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment," *J. Netw. Comput. Appl.*, 2017, vol. 89, pp. 72–85.
[68] F. Wu *et al.*, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Generation Comput. Syst.*, vol. 82, pp. 727–737, 2018.
[69] L. Xiong, D. Peng, T. Peng, H. Liang, and Z. Liu, "A lightweight anonymous authentication protocol with perfect forward secrecy for wireless sensor networks," *Sensors*, vol. 17, no. 11, 2017, Art no. 2681.
[70] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic iot networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.
[71] P. K. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for internet of things environments," *Int. J. Commun. Syst.*, vol. 30, no. 16, 2017, Art no. e3323.
[72] Y. Lu, L. Li, H. Peng, and Y. Yang, "An energy efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks," *Sensors.*, vol. 16, no. 6, 2016, Art no. 837.
[73] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Security Commun. Netw.*, vol. 9, no. 16, pp. 3670–3687, 2016.
[74] B. Vaidya, D. Makrakis, and H. Mouftah, "Two-factor mutual authentication with key agreement in wireless sensor networks," *Security Commun. Netw.*, vol. 9, no. 2, pp. 171–183, 2016.
[75] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Comput. Syst.*, vol. 80, pp. 483–495, 2018.
[76] X. Li, J. Niu, and K.-K. R. Choo, "A robust authentication protocol with privacy protection for wireless sensor networks," in *Proc. 12th Int. Workshop Radio Freq. Identification Internet Things Security, 2016*, pp. 30–44.
[77] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, "An efficient biometric authentication protocol for wireless sensor networks," *Int. J. Distrib. Sensor Netw. 2013*, pp. 1–13.
[78] T.-C. Hsiao, Y.-T. Liao, J.-Y. Huang, T.-S. Chen, and G.-B. Horng, "An authentication scheme to healthcare security under wireless sensor networks," *J. Med. Syst.*, vol. 36, no. 6, pp. 3649–3664, 2012.
[79] P. Kumar, A. J. Choudhury, M. Sain, S.-G. Lee, and H.-J. Lee, "Ruasn: A robust user authentication framework for wireless sensor networks," *Sensors J.*, vol. 11, no. 5, pp. 5020–5046, 2011.
[80] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors J.*, vol. 11, no. 5, pp. 4767–4779, 2011.
[81] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks." *Ad Hoc Sens. Wireless Netw.*, vol. 10, no. 4, pp. 361–371, 2010.
[82] T.-H. Chen and W.-K. Shih, "A robust mutual authentication protocol for wireless sensor networks," *ETRI J.*, vol. 32, no. 5, pp. 704–712, 2010.
[83] J. Yuan, C. Jiang, and Z. Jiang, "A biometric-based user authentication for wireless sensor networks," *Wuhan Univ. J. Nat. Sci.*, vol. 15, no. 3, pp. 272–276, 2010.
[84] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1382–1392, Jun. 2017.
[85] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment," *IEEE Trans. Depend. Sec. Comput.*, to be published.
[86] G. M. Yang, D. S. Wong, H. X. Wang, and X. T. Deng, "Two-factor mutual authentication based on smart cards and passwords," *J. Comput. Syst. Sci.*, vol. 74, no. 7, pp. 1160–1172, 2008.
[87] I. Liao, C. Lee, and M. Hwang, "A password authentication scheme over insecure networks," *J. Comput. Syst. Sci.*, vol. 72, no. 4, pp. 727–740, 2006.
[88] R. Madhusudhan and R. C. Mittal, "Dynamic id-based remote user password authentication schemes using smart cards: A review," *J. Netw. Comput. Appl.*, vol. 35, no. 4, pp. 1235–1248, 2012.

Ding Wang (M'17) received the Ph.D. degree in information security from Peking University, Beijing, China, in 2017.

He has published more than 40 papers at venues, such as ACM Conference on Computer and Communications Security, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, and the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. His research focuses on user authentication.

Wenting Li received the M.E. degree from School of Software and Microelectronics, Peking University, Beijing, China, in 2016. She is currently working toward the Ph.D. degree in information security with Peking University. Her research focuses on authentication protocol.

Ping Wang (M'88–SM'16) received the doctorate degree in computer science from the University of Massachusetts, Lowell, MA, USA, in 1996.

He is currently a Professor with Peking University, Beijing, China. He has authored or co-authored more than 70 papers in journals or proceedings such as IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, ACM Conference on Computer and Communications Security, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. His research interests include Internet of things, distributed computing, and information security.