An Enhanced Temporal-Credential-Based Mutual Authentication and Key Agreement Scheme for Wireless Sensor Network

Muxi Zhang and JooSeok Song

Abstract—**Sometimes, people want to get real-time sensory information from many domains such as medical monitoring, disaster detection and military surveillance. To achieve this, wireless sensor network (WSN) is a useful tool. A legitimate user can login to the network and access the sensory data from legitimate sensor nodes with the aid of gateway node. Since WSN is an energy-constrained environment, a secure and lightweight authentication scheme among user, gateway node and sensor node is important in WSN. In this paper, a secure mutual authentication and key agreement (MAAKA) scheme for WSN which improves three related works is suggested. Compared with them, the proposed scheme is more secure. It also reduces the total computational overhead by at least 13.6% while almost maintaining the communication overhead.**

Index Terms—**Key agreement, mutual authentication, temporal credential, wireless sensor network.**

I. Introduction

Wireless sensor network (WSN) is a useful tool to collect sensory information from places with the support of distributed sensor nodes. It can be used in many fields such as military, e-health, environment monitoring and natural disaster detection [1]-[9]. In WSN, there are many sensor nodes with limited energy, communication capability and computational capability. The data from sensor nodes are collected by a gateway node and then transferred to a legitimate user. In many cases, WSN is often deployed in an unattended environment [1]-[13] and an attacker can easily threaten the security of it (e.g. impersonating a sensor node or launching tracking attack). Thus, a secure and lightweight entity authentication model is very important in WSN. After being authenticated by the gateway node, a legitimate user and a legitimate sensor node are allowed to establish a real-time communication channel between them. To secure this channel, more and more works choose to perform the two-factor authentication with the help of a smartcard. It is because that the information stored in the smartcard is difficult to be replicated or extracted [12], [14]. Additionally, with a portable smartcard storing the credential and other important values, it is convenient to perform authentication anywhere. During entity authentication, the following security requirements should be met: anonymity, session key generation and attack resistance [3]. However, recent works using smartcard [2]-[4] were found that they cannot meet all of them and suffer from several security problems like tracking attack, lost smartcard attack. They also lack secure password update phase and are weak in information integrity checking.

In this paper, an enhanced temporal-credential-based mutual authentication and key agreement scheme for resource-constrained WSN is proposed. The proposed scheme uses only XOR and hash function with the help of smartcard. Users and sensor nodes first register on a gateway node and then get their temporal credential. User will also get a personalized smartcard from the gateway node which stores some other sensitive values besides his/her temporal credential. After registration, user and sensor node will perform the indirect mutual authentication with the aid of the gateway node. They exchange their private key to finally share a session key. In the proposed scheme, the problems in [2]-[4] are fixed while maintaining the communication overhead and reducing the computational overhead.

The rest of the paper is organized as follows: Section II briefly reviews the related works and summarizes the important points that need to be considered while designing an entity authentication scheme for WSN. Section III presents the scheme, and then Section IV provides performance analysis and comparison with the related works. Finally, Section V concludes this paper.

II. Related Works

There were many subsequent schemes [1-8, 10, 13] proposed since Das *et.al* [12] presented the first work on two-factor user authentication in WSN using smartcard. Among them, Xue *et.al.* [1] designed a temporal-credential-based mutual authentication and key agreement (MAAKA) scheme which has high efficiency since it only uses XOR and hash function. Then several papers [2]-[4] pointed out some weaknesses in [1] and proposed schemes with better security and performance. However, a few similar mistakes were repeated in them. Li *et al*.'s scheme [2] cannot resist to off-line guessing attack, modification attack and tracking attack. It also lacks password update phase, without which password stays static and is more vulnerable to off-line password guessing attack [9]. The work of He *et.al* [3] is vulnerable to sensor impersonation attack and tracking attack. Like Li *et al*.'s work, it fails to support password update too. In Jiang *et al*.'s scheme [4], while

Manuscript received March 11, 2018; revised May 10, 2018. This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2015R1D1A1A01058928).

Muxi Zhang and JooSeok Song are with the Department of Computer Science, Yonsei University, Seoul, CO 03722 South Korea (e-mail: zmx0825@gmail.com, jssong2526@yonsei.ac.kr).

doi: 10.18178/jacn.2018.6.1.250

tracking problem is resolved, de-synchronization problem happens [11]. In [4], user's identity is updated during every authentication session on both user and GWN side to resist to the tracking attack. However, the synchronization of the update of user's identity may not be ensured due to the network congestion or a malicious delay. This causes the de-synchronization problem and makes user easily be blocked out of the system. This work is also vulnerable to lost smartcard problem and has no secure password check mechanism which can be abused by an attacker to launch a Denial of Service (DoS) attack.

To resolve the security problems in [2]-[4], namely the lack of secure password update phase, tracking problem, off-line guessing problem and lost smartcard problem, and modification problem, the following security requirements should be met:

1) Support secure password update: It is necessary to have a user-friendly password update mechanism to allow user to change their passwords freely. Before updating password, the mechanism must also ensure that the submitted old password is correct otherwise a malicious person can abuse this to block a legitimate user out (i.e. launching a DoS attack).
2) Use dynamic temporary identity (TID): The TID of user used in each authentication session should be different to resist tracking attack.
3) Add 'salt': To resist to off-line guessing attack, some 'salt' (i.e. a big random number r_i) should be concatenated or XORed with the sensitive information (e.g. user's password). It is assumed that the 'salt' is hard to be guessed within the limitation of transmission delay. Meanwhile, to resist lost smartcard attack, 'salt' should also be added to the data stored in the smart card [11].
4) Ensure integrity: To detect modification attack, integrity checking is needed since in most of the situations network is a public environment. Once something is modified, it should be detected immediately and any entity can terminate the current session and start a new one.

III. Proposed Scheme

This section describes an enhanced temporal-credential-based MAAKA scheme for WSN using only XOR and one-way hash function based on [2]-[4]. There are three entities: user (U), sensor node (SN) and gateway node (GWN). The purpose of the scheme is establishing a real-time communication channel between U and SN with GWN working as a bridge in the middle (see Fig. 1).

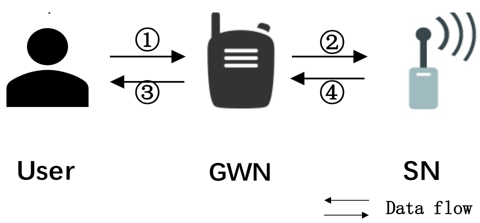

Fig. 1. System model.

While taking the WSN in a medical environment for example, U is a doctor while SNs are the medical sensors set on a patient. First of all, a doctor should register with the GWN and get his/her smartcard. In general cases, this doctor only has access to the sensory data (e.g. blood pressure, heart rate) of those patients who he/she is responsible for. SNs also need to do the registration with GWN to obtain their temporal credentials. Then, when need, the doctor can use his/her smartcard to login to the GWN. After verifying the legality of the doctor, GWN collects the sensory data from the SNs in its cluster and sends them back to the doctor. In this way, a legitimate doctor can monitor the health condition of his/her patients remotely. This scheme also allows the doctor to change his/her password whenever he/she wants.

The scheme consists of three phases: registration phase, login and authentication phase and password update phase. The notations used in the paper are summarized in Table I.

A. Registration Phase

This phase comprises two parts: user registration and sensor node registration. They are illustrated as Fig. 2 and Fig. 3 respectively, and more details will be introduced as follows.

TABLE I: Notation Description

Notation	Description
ID_i; PW_i	The identity and password of U_i
SID_j	The identity of SN_j
PTC_i; PTC_j	The protected temporal credential of U_i and SN_j
C_i; C_{GWN}; C_j	Confirm information generated by U_i, GWN and SN_j separately
$K_{GWN\text{-}U}$; $K_{GWN\text{-}SN}$	Private key only known to GWN while communicating with U_i or SN_j
K_i; K_j	Keys generated by U_i and SN_j separately
PKS_i; PKS_{GWN}; PKS_j	Security information to protect keys generated by U_i, GWN or SN_j
TC_i; TC_j	The temporal credential of U_i or SN_j
VI_i; VI_j	The verification information of U_i and SN_j
TS	Timestamp
TE_i	The expiration time of the TC_i
$H(\bullet)$	A one-way hash function
$\|\|$	The bitwise concatenation operation
$\oplus$	The bitwise XOR operation

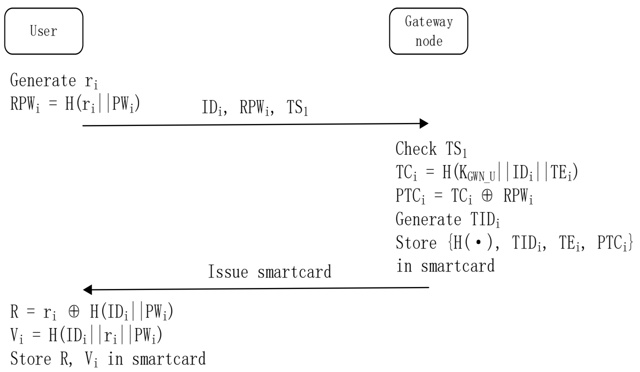

Fig. 2. Registration phase for user.

1) Registration phase for user

Before registration, the real identity of the user should be checked. If the user is authorized (thinking about the doctor who only has access to the sensors set on his patients but not those on other patients), he/she can register the certain GWN.

1) U_i selects an unique ID_i and PW_i, generates a random value r_i and computes $RPW_i = H(r_i \parallel PW_i)$. Then U_i generates a timestamp TS_1 and sends registration request message $\{ID_i, RPW_i, TS_1\}$ to GWN.
2) Upon receiving the request message, GWN first checks the freshness of TS_1. If it is valid, GWN calculates U_i's temporal credential $TC_i = H(K_{GWN\text{-}U} \parallel ID_i \parallel TE_i)$ and $PTC_i = TC_i \oplus RPW_i$. Then GWN generates a unique TID_i randomly and stores it securely in an identity table (Table II) with U_i's ID_i, Count, TE_i and Status-bit in GWN's database. The Status-bit is used to record whether a user has already logged in (i.e. 1 for logged in and 0 for not logged in). the Count which is a random value generated by GWN will be used later when update TID_i in authentication phase to resist tracking attack. At last, GWN personalizes a smartcard for U_i with $\{H(\bullet), TID_i, TE_i, PTC_i\}$ stored in it and sends it to U_i in a secure way.
3) After receiving the smartcard, U_i firstly computes $R = r_i \oplus H(ID_i \parallel PW_i)$ and $V_i = H(ID_i \parallel r_i \parallel PW_i)$ and then stores them in smartcard additionally.

2) Registration phase for sensor node

First of all, it is assumed that a large random number r_j pre-shared between SN_j and GWN.

1) SN_j generates a timestamp TS_2 and sends its SID_j with TS_2 to GWN.
2) GWN checks the freshness of TS_2. If TS_2 is valid, GWN obtains r_j according to SID_j and does the calculations as $TC_j = H(K_{GWN\text{-}SN} \parallel SID_j)$, $PTC_j = TC_j \oplus r_j$ and $V_j = H(r_j \oplus PTC_j)$. At last, a response $\{PTC_j, V_j, TS_3\}$ is sent back to SN_j.
3) Upon receiving $\{PTC_j, V_j, TS_3\}$, if TS_3 is valid, SN_j calculates $V_j^* = H(r_j \oplus PTC_j)$ and compares it with V_j. If $V_j^* = V_j$, SN_j stores $TC_j = PTC_j \oplus r_j$; otherwise, something may be modified and SN_j can halt the current registration phase.

TABLE II. IDENTITY TABLE

TID_i	ID_i	Count	TE_i	Status-bit
***	***	***	***	0/1

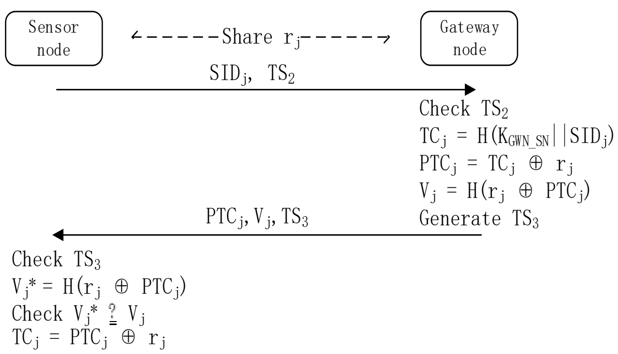

Fig. 3. Registration phase for sensor node.

B. Login and Authentication Scheme

When a user wants to ask for some information from sensors, the user needs to be authenticated. Count is used here to calculate $TID_i^* = TID_i + \text{Count}$. In this way, even in the same authentication session the TID_i^* used on GWN and SN_j side is different from TID_i. As a result, an attacker who wants to launch a tracking attack following the user's TID_i value will fail. Additionally, to prevent the de-synchronization problem in [4], TID_i is only dynamic on GWN and SN side.

The following steps will be executed in login and authentication phase (see Fig. 4).

1) U_i inserts the smartcard in a terminal and enters identity ID_i and password PW_i, using which smartcard can extract r_i from R as $r_i = R \oplus H(ID_i \parallel PW_i)$. After generating a timestamp TS_4 and a random private key K_i, U_i computes the temporal credential $TC_i = PTC_i \oplus H(r_i \parallel PW_i)$, $C_i = H(ID_i \parallel TS_4 \parallel K_i) \oplus TC_i$ and $PKS_i = K_i \oplus H(TC_i \parallel TS_4)$. At last, message $\{TID_i, PKS_i, C_i, TS_4\}$ will be sent to GWN.
2) If TS_4 is valid, GWN obtains U_i' s ID_i that stored in identity table according to TID_i. Then GWN calculates $TC_i^* = H(K_{GWN\text{-}U} \parallel ID_i \parallel TE_i)$, $K_i^* = PKS_i \oplus H(TC_i^* \parallel TS_4)$ and checks whether $C_i^* = H(ID_i \parallel TS_4 \parallel K_i^*) \oplus TC_i^*$ equals to C_i. If $C_i^* = C_i$, GWN authenticates U_i successfully. After that, Count is generated randomly and updated in identity table. The value of TID_i^* is calculated as TID_i + Count. Then, GWN generates SN_j' s temporal credential $TC_j = H(K_{GWN\text{-}SN} \parallel SID_j)$ and TS_5, computes $C_{GWN} = H(TID_i^* \parallel TC_j \parallel TS_5)$, $PKS_{GWN} = K_i \oplus H(TC_j \parallel TS_5)$ and sends $\{TID_i^*, C_{GWN}, PKS_{GWN}, TS_5\}$ to SN_j.
3) After verifying the freshness of TS_5, SN_j computes $C_{GWN}^* = H(TID_i^* \parallel TC_j \parallel TS_5)$ and compares it' s value with C_{GWN}. If they are equal, GWN is believed to be a legitimate gateway node and it is believed that no data have been modified during transmission. SN_j will then extract K_i from PKS_{GWN} by calculating $K_i = PKS_{GWN} \oplus H(TC_j \parallel TS_5)$. After that, SN_j randomly generates its private key K_j and a timestamp TS_6, computes $C_j = H(K_j \parallel TID_i^* \parallel SID_j \parallel TS_6)$, $PKS_j = K_j \oplus H(K_i \parallel TS_6)$. Finally, it sends SID_j, C_j, PKS_j with TS_6 to GWN.
4) If the check of the freshness of TS_6 is passed, GWN computes $K_j = PKS_j \oplus H(K_i \parallel TS_6)$, $C_j^* = H(K_j \parallel TID_i^* \parallel SID_j \parallel TS_6)$. If $C_j^* = C_j$, it continues to generates a new timestamp TS_7 and computes $C_j' = H(K_j \parallel (TID_i^* - \text{Count}) \parallel SID_j \parallel TS_6)$. Eventually, GWN transfers SID_j, C_j', PKS_j, TS_6 and TS_7 to U_i.
5) Upon receiving the message, U_i first checks TS_7 and does the same operations as GWN in step 4) with C_j' replacing C_j and TID replacing TID_i^*. However, the last operation that computes C_j' is not needed on user side.
6) Finally, session key is shared by U_i and SN_j as $KEY_{ij} = H(K_i \oplus K_j)$.

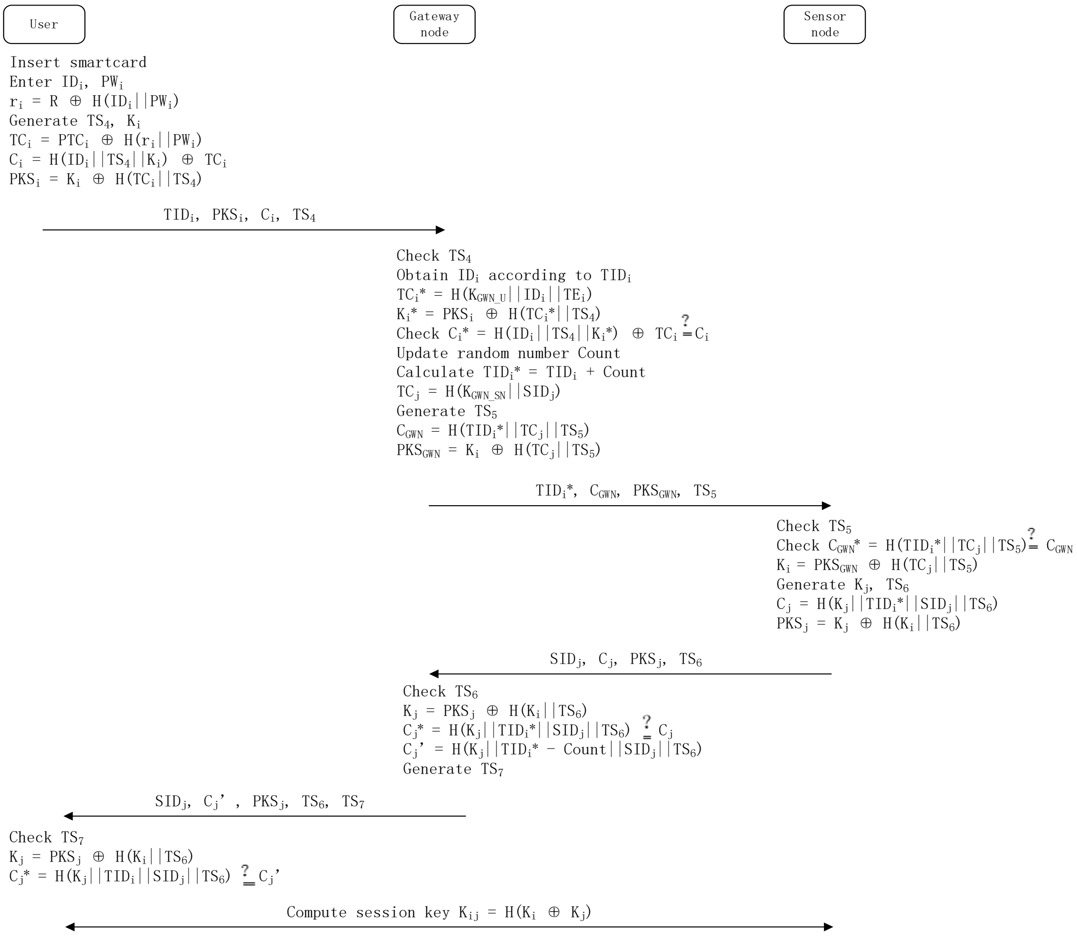

Fig. 4. Login and authentication phase.

C. Password Update Phase

When a user wants to change his/her password, the following mechanism will be started (see Fig. 5). U_i inserts smartcard to a terminal and submits ID_i, PW_i^{old} and PW_i^{new}. Then r_i is extracted as $r_i = R \oplus H(ID_i \parallel PW_i^{old})$ and used to calculate $V_i^* = H(ID_i \parallel r_i \parallel PW_i^{old})$. If $V_i^* = V_i$, $R^{new} = r_i \oplus H(ID_i \parallel PW_i^{new})$ and $V_i^{new} = H(ID_i \parallel r_i \parallel PW_i^{new})$ will be updated; else user's update request will be refused.

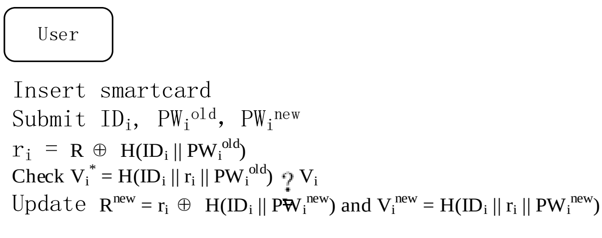

Fig. 5. Password update phase.

IV. Security and Performance Evaluation

This section is divided into two parts, one is security analysis and the other is performance comparison with related works.

A. Security Analysis

1) Resistance to lost smartcard problem: The threat model for lost smartcard problem is that an attacker M obtains the smartcard of user and recovers the secret parameters $\{H(\cdot), TID_i, TE_i, PTC_i, V_i, R\}$ stored in it (e.g. by differential power analysis [14]). However, to get the random value r_i generated by U, M must know both U's ID_i and PW_i which is hard in the scheme. Without r_i, none of other sensitive information (i.e. TC_i) can be extracted. TC_i cannot also be calculated by M directly since M does not have the private key $K_{GWN\text{-}U}$ which is only known to GWN. In conclusion, the proposed scheme can resist to lost smartcard attack.

2) Resistance to tracking attack without de-synchronization problem: Tracking attack means that an attacker M can track the user's identity to get something meaningful related to the user such as access pattern to interested sensors. In this scheme, to resist to tracking attack, TID_i is updated for every authentication session on GWN and SN side. An attacker who eavesdrops TID_i from user's login request message in the early session may notice when a user attempts to log in. However, TID_i is transformed to TID_i^* on GWN and SN side and they are totally different values. Thus, it is hard for the attacker to track the user's identity to know with which SN the same user communicates. In addition, since TID_i is fixed on user side, there will be no de-synchronization problem due to the de-synchronous update of TID_i on GWN and user side. Thus, the proposed scheme is free from tracking attack as well as de-synchronization attack.

3) Support for secure password update: the scheme checks the old password by computing $V_i^* = H(ID_i \parallel r_i \parallel PW_i^{old})$ and comparing it with the value V_i stored in the smartcard before updating the password. If they are equal, password

update will be allowed. This mechanism prevents attackers from inputting any old password to update it and finally causing a DoS problem to the user.

4) Support for integrity check: Due to the usage of public channel, entities are vulnerable to modification attack. The sensitive data (e.g. TC_i for user) can be modified during transmission, which may cause severe security problems. The proposed scheme checks the integrity of the received messages at each step using V_j, C_i, C_{GWN} or C_j. If any abnormity is detected, the current session will be halted and a new session can be started.

B. Performance Comparison

In this section, a comparison between the proposed scheme and [2]-[4] will be shown in terms of the security functionality, communication overhead and computational overhead. Table III shows that the related schemes cannot support every security functionality but the proposed scheme can. Here in Table III, '-' means that there is no meaning to consider the functionality in a certain scheme.

Since the registration phase for each user as well as for each sensor node is only executed once, it will not be considered in the comparison of communication and computational overhead. There may be some overhead (3-4 T_h, T_h means the computational time for hash function while XOR's computational time can be ignored [3]) caused by additional password update phase but this phase is not played frequently (e.g. only once per month), it will not be considered in the evaluation either. In other words, only the costs introduced in the login and authentication phase are taken into account.

The communication costs of the proposed scheme and the related works for a successful authentication are summarized in Table IV. The proposed scheme requires 4 message exchanges which is the same as [2] and [4] while [3] requires 3 message exchanges. Although it needs one more message exchange than [3], it resolves the security problems in [3] such as tracking attack. With almost the same communication cost, the proposed scheme can do better than any relate work in security.

As seen from Table V, the total computational overhead of the proposed scheme is 7 T_h, 4 T_h and 3 T_h less than others, which achieves a 26.9%, 17.3% and 13.6% improvement on computational performance respectively. In conclusion, the proposed scheme is safer and more efficient.

TABLE III. SECURITY FUNCTIONALITY COMPARISON

Functionality	Li et.al [2]	He et.al [3]	Jiang et.al [4]	Proposed scheme
Mutual authentication	Yes	Yes	Yes	Yes
Key agreement	Yes	Yes	Yes	Yes
Resistance to off-line guessing attack	No	No	No	Yes
Resistance to lost smartcard problem	Yes	Yes	No	Yes
Resistance to tracking attack	No	No	Yes	Yes
Resistance to de-synchronization problem	-	-	No	Yes
Secure password update	No	No	No	Yes
Integrity check	Not for all phases	Yes	-	Yes

TABLE IV. COMMUNICATION COST COMPARISON

Scheme	Communication cost
Li *et.al* [2]	4 messages
He *et.al* [3]	3 messages
Jiang *et.al* [4]	4 messages
Proposed scheme	4 messages

TABLE V. COMPUTATIONAL OVERHEAD COMPARISON

Entity	Li et.al [2]	He et.al [3]	Jiang et.al [4]	Proposed scheme
SN	6 T_h	7 T_h	5 T_h	4 T_h
U	9 T_h	6 T_h	7 T_h	6 T_h
GWN	11 T_h	10 T_h	10 T_h	9 T_h
Total	26 T_h	23 T_h	22 T_h	19 T_h

V. CONCLUSION

This paper proposes an enhanced temporal-credential-based MAAKA scheme. In the scheme, user and sensor node perform the indirect mutual authentication with the aid of the gateway node and finally share a session key. Compared to the existing schemes, the proposed scheme can resist to tracking attack and lost smartcard attack, and support secure password update phase and information integrity checking. It also achieves a better performance in total computational time. Recently, many elliptic-curve-cryptography-based [5], [13], [15], [16] and biometric-based [6] works have been proposed. It is considered that they may cause more overhead on SNs due to their intrinsic complexity. However, these technologies draw more and more attention these days so the comparison with those schemes will be left as future work.

ACKNOWLEDGMENT

One of us (Zhang. Song.) would like to thank those who helped us during the writing of this paper, namely Inhwan Kim, Jaehyu Kim, Hyoungmin Ham and Bosung Kim. They give us many useful academic and constructive advices, and also help us to correct the paper.

REFERENCES

[1] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 1, pp. 316-323, 2013.

[2] 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*, vol. 8, pp. 9589-9603, 2013.

[3] 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," *Information Sciences*, vol. 321, pp. 263-277, 2015.

[4] 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 Networking and Applications*, vol. 6, pp-1070-1081, 2015.

[5] 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 Networking and Applications*, vol. 1, pp. 16-30, 2017.

[6] X. Li, Journal of network and computer applications. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2017.07.001

[7] 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 Networks,* vol. 20, pp. 96-112, 2014.

[8] 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,* vol. 4, pp. 6443-6462, 2014.

[9] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Networks,* vol. 27, pp. 159-194, 2015.

[10] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-to-peer Networking and Applications*, vol. 1, pp. 223-244, 2016.

[11] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks" *Ad Hoc Networks,* vol. 20, pp. 1-15, 2014.

[12] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications,* vol. 3, pp. 1086-1090, 2009.

[13] 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," *Journal of Network and Computer Applications*, vol. 76, pp. 37-48, 2016.

[14] M. Cobb and J. Meckley, Smartcard, *TechTarget.* [Online]. Available: http://searchsecurity.techtarget.com/definition/smart-card

[15] 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,* vol. 6, pp. 10081-10106, 2014.

[16] Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He, and N. Chilamkurti, "A privacy - aware two - factor authentication protocol based on elliptic curve cryptography for wireless sensor networks," *International Journal of Network Management*, vol. 3, 2017.

Muxi Zhang was born in Beijing, China on August 25th, 1994. She received the B.S. degree in software engineering from Sun Yat-sen University, Zhuhai, China, in 2016. She is currently working toward the M.S. degree in computer science at Yonsei University, Seoul, Republic of Korea. Her research interests include secondary authentication and mutual authentication and key agreement in wireless sensor network.

JooSeok Song received the B.S. degree in Electrical Engineering from Seoul National University, Seoul, Korea, in 1976, and the M.S. degree in electrical engineering from Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 1979. In 1988, he received the Ph.D degree in computer science from University of California at Berkeley. From 1988 to 1989, he was an assistant professor at the Naval Postgraduate School, Monterey, CA. He was the president of Korea Institute of Information Security and Cryptology in 2006. He is currently a professor of computer science at Yonsei University, Seoul. His research interests include cryptography and network security.