A Secure Three Party Node Authentication and Key Establishment Scheme for the Internet of Things Environment

Chun-Ta Li[1], Cheng-Chi Lee[2], Chi-Yao Weng[3]

[1] Department of Information Management, Tainan University of Technology, Taiwan
[2] Department of Library and Information Science, Fu Jen Catholic University, Taiwan
Department of Photonics and Communication Engineering, Asia University, Taiwan
[3] Department of Computer Science, National Pingtung University, Taiwan
th0040@mail.tut.edu.tw, cclee@mail.fju.edu.tw, cyweng@mail.nptu.edu.tw

Abstract

Secure three party node authentication and key establishment scheme for data exchange in the Internet of Things (IoT) applications enables two resource-constrained nodes to establish a secure end-to-end communication channel with the help of a data server. Since node in IoT have constraints on resources such as power, memory space and computation ability. Thus may existing key establishment schemes are unable to run IoT applications and many researchers are already working on how to integrate new techniques and efficient approaches into the IoT environment. Recently, Nasiraee and Mohasefi proposed a highly efficient and novel key establishment scheme for Internet-Enable Sensor Networks (IESN) which was adapted to the IoT notion. Nasiraee-Mohasefi's scheme presented a novel approach where a new node that joins the IoT network is responsible to aggregate interested neighbors' information and to send a request to the trusted server to get required pairwise session keys. However, we found that Nasiraee-Mohasefi's scheme has some security and efficiency shortcomings and this paper focuses on preventing the above-mentioned weaknesses of Nasiraee-Mohasefi's scheme by proposing an improved three party node authentication and key establishment scheme. The results of security proof by BAN logic analysis confirms the proposed scheme provides a considerable gains in power saving while its security properties are ensured for the Internet of Things environment.

Keywords: Authentication, Cryptanalysis, Internet of Things, Three party key establishment.

1 Introduction

In the Internet of Things (IoT) notion [1, 33, 35, 36, 39], the interconnected objects (i.e. smart devices, RFID tags, sensors and vehicles) are seamlessly integrated into networks for providing intelligent services and new applicative perspectives on our everyday lives, such as RFID applications [16, 21], Ad hoc networks [19], Wireless Sensor Networks (WSN) [9, 11, 20, 34], Vehicular Ad hoc Networks (VANET) [4, 15, 17, 37, 40], Wireless Body Area Networks (WBAN) [13, 41], and so on. In general, a IoT environment is consists of three parts including sensing and monitor unit, data aggregation and transmission, and intelligent computing. Various services of IoT have been emerging into markets in wide areas such as mobile emergency medical care system, entrance guard management system, intelligent transportation control system, and remote healthcare monitoring system. Considering social, ethical and legal aspects of IoT systems, data collected by sensing unit might be highly sensitive and should be managed properly to guarantee user privacy and information security [3, 5, 8, 10, 12, 18, 38]. In the last decade, there have been several studies and surveys [6, 7, 22-25, 29, 30] provide different security threats and privacy concerns while collecting, transmitting, processing and storing data.

In order to protect the security of Internet of Things, a three party key establishment approach provides a convenient way to secure end-to-end communication environments and allows two nodes establish a secure channel via the help of the trusted server. As introduced in [27, 32], existing security solutions for IoT is categorized into two types: asymmetric key schemes and symmetric key pre-distribution schemes. The asymmetric key schemes are widely deployed in key transport and key agreement. However, the applicability of using asymmetric key schemes in the context of IoT still one major disadvantages, which is power consumption and expensive computations. In contrast with asymmetric key schemes, symmetric key pre-distribution schemes assume that nodes involved in the key establishment share a symmetric key or some random bytes flashed into the device before its deployment. An Internet Enabled Sensor Networks (IESN) is an important part of the IoT and Figure 1 demonstrates key establishment phase of sensor nodes

*Corresponding Author: Cheng-Chi Lee; E-mail: cclee@mail.fju.edu.tw
DOI: 10.3966/160792642018011901014

in the scenario of IESN architecture [32]. Due to tiny sensors are resource constrained on limited processing ability, transmission range and battery life, this paper will aim to present a pre-distribution symmetric key based three party node authentication and key establishment scheme for IESN. In the following, we shortly review some previous works for trusted party based three party authentication scheme.

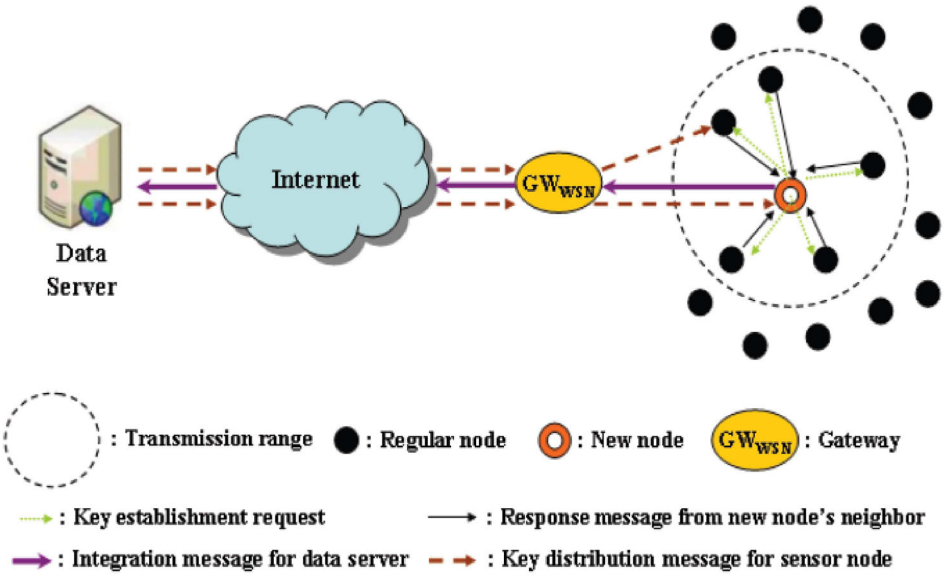

Figure 1. Internet enabled sensor networks architecture [32]

In 1993, MIT proposed a well-known three party authentication scheme called Kerberos [14], which is based on TCP/IP protocol stack and uses some features such as using timestamps and providing time-synchronization, which cause serious problem for IoT and IESN. In 2002, Perrig et al. proposed a secure network encryption protocol called SNEP [28], which needs a trusted third party to establish shared secret between two nodes. However, Nasiraee and Mohasefi [26] introduced SNEP method has a kind of Denial-of-Service (DoS) vulnerability, which caused nodes to waste power and significant reduce the lifetime in sensor networks. In order to satisfy essential security and efficient metrics for IESN, in 2015, Nasiraee and Mohasefi further proposed an efficient three party key establishment scheme with DoS and Sybil attacks resistance. Their solution reduces energy consumption about 75% vs. SNEP, which causes a significant increase in lifetime of nodes. Unfortunately, we found that Nasiraee-Mohasefi's three party key establishment scheme may suffer from session key disclosure attack. The spotted security weakness may allow a malicious attacker to use the stolen/compromised pseudo random function to derive any pairwise session key shared between two nodes and the back-end server is not aware of having caused this problem. In addition, their scheme exhibits a low efficiency problem during authentication procedure, which leads to a significant waste of power and lifetime in sensor nodes. To repair these two weaknesses, we present a more secure three party node authentication and key establishment scheme with the same advantages for IESN.

The remainder of the paper is organized as follows. Section 2 provides a brief review of Nasiraee-Mohasefi's scheme, whereby the weaknesses of the reviewed scheme are presented in Section 3. Section 4 presents our new proposed scheme which removes the weaknesses of Nasiraee-Mohasefi's scheme. We present the security proof of the proposed scheme in Section 5. Finally we conclude this paper in Section 6.

2 Review of Nasiraee-Mohasefi's Scheme

In this section, Nasiraee-Mohasefi's scheme [26] will be briefly reviewed. There are four phases in Nasiraee-Mohasefi's scheme: key establishment request, response message, construction of message type 3, and operations in the server *S*. For convenience of description, terminology and notations used in the paper are summarized in Table 1.

We assume that the new node *A* wants to join the IoT network by establishing shared secrets with its neighbors including the node *B*. Figure 2 shows the flowchart of Nasiraee-Mohasefi's scheme and the process is done as follows:

Table 1. Notations used in the paper

Symbol	Description
A, B	Node A and node B
S	The server
ID_A	The identity of node A
ID_B	The identity of node B
K_{SA}	A secret key known only to S and A
K_{SB}	A secret key known only to S and B
K_{AB}	A symmetric session key shared between S and B
	Two nonces which are generated by node A
$N1_A$, $N2_A$	A nonce which is generated by node B
N_B	A set of pairs of identifiers and nonces of
$NeiSet_A$	the interested neighbors of node A
	A message authentication code, such as
$MAC(.)$	HMAC [31]
	Symmetric key encryption with key K
$\{.\}_K$	A pseudo random function which has enough
$f(.)$	security for constructing a symmetric key
	session key
$\|$	Message concatenation

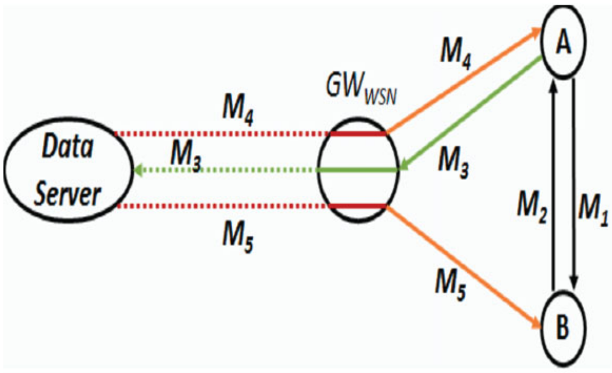

Figure 2. The flowchart of Nasiraee-Mohasefi's scheme

Phase 1: Key Establishment Request

In this phase, IoT nodes will start secure communication among themselves. When a new node A wants to join the network, A is required to generate a request message $M_1 = ID_A \| N1_A$ and M_1 is locally broadcast to interested neighbors, where $N1_A$ is a nonce generated by A.

Phase 2: Response Message

In this phase, all interested neighbors in the transmission range of the node A that receive M_1, such as the node B, B will locally broadcast response message $M_2 = ID_A \| ID_B \| N1_A \| N_B$, where N_B is a nonce generated by B.

Phase 3: Construction of Message Type 3

After receiving all response messages of type M_2, the new node A constructs a message type 3, $M_3 = ID_A \| N2_A \| NeiSet_A \| MAC(K_{SA}, ID_A \| N2_A \| NeiSet_A)$ and transmits it to the server S, which is in communication range. Note that the identifiers in $NeiSet_A$ show the neighbors of A that are interested to establish a pairwise session key with A and node A concatenates a nonce $N2_A$ to provide strong freshness of message M_3.

Phase 4: Operations in the Server *S*

After receiving M_3 from node A, the server S checks replay attacks on M_3 by $N2_A$. For simplicity, we have only mentioned the node B. S establishes a pairwise session key K_{AB} shared between A and B by computing $K_{AB} = f(ID_A \| ID_B \| N2_A)$, where K_{AB} would be done by a pseudo random function $f(.)$, which has enough security. After generating K_{AB}, messages M_4 and M_5 would be constructed as follows:

$$M_4 = \{K_{AB}\}_{K_{SA}} \| MAC(K_{SA}, K_{AB} \| ID_B \| N2_A)$$
$$M_5 = \{K_{AB}\}_{K_{SB}} \| MAC(K_{SB}, K_{AB} \| ID_A \| ID_B)$$

After generating messages M_4 and M_5, server S unicasts them to the corresponding node A and its neighbor node B. The nodes after receiving M_4 and M_5 (checking integrity, authentication and freshness), use the included shared session key, K_{AB}, to securely communicate. Note that other IoT nodes are unaware about K_{AB}, because they do not have K_{SA} and K_{SB}.

3 Weaknesses of Nasiraee-Mohasefi's Scheme

In this section, we highlight two weaknesses of Nasiraee-Mohasefi's scheme. The details of two weaknesses are described in the following subsections.

3.1 Insecurity of A Pseudo Random Function *f*(.)

In Nasiraee-Mohasefi's scheme, we observe the insecurity of a pseudo random function $f(.)$. Assume the pseudo random function $f(.)$ is compromised by the attacker C, he/she can use this function to compute any pairwise session key between two nodes. The detailed steps are presented as follows:

Step 1. The attacker C steals the pseudo random function $f(.)$ from S.

Step 2. The attacker C eavesdrops the message type 3, M_3 from IoT network and knows ID_A, $N2_A$, and $NeiSet_A = (ID_X \| N_X \| \ldots)$, where $X = 1, 2, 3, \ldots, n$ and n is the number of neighbors of A that are interested to establish a shared pairwise key with A.

Step 3. After getting $f(.)$ and M_3, C can easily compute any shared pairwise session key $K_{AX} = f(ID_A \| ID_B \| N2_A)$ between node A and node X without knowing K_{SA} and K_{SX}.

From above-mentioned steps show, the attacker may launch this attack and Nasiraee-Mohasefi's scheme cannot prevent session key disclosure attacks.

3.2 Low Efficiency in Phase 4 of Nasiraee-Mohasefi's Scheme

When the server S unicasts a response message M_4 to node A, A verifies the authenticity of pairwise session key by decrypting $\{K_{AX}\}_{K_{SA}}$, where $X = 1, 2,$

3, …, n. If the shared pairwise key K_{AX} is revealed, A is unable to know which neighbor node did A share with. Therefore A may compute n times $MAC'(K_{SA}, K_{AX}||ID_X||N2_A)$ at most and compares them with some neighbor node. In this case, we suppose the node A takes j milliseconds to compute one $MAC'(K_{SA}, K_{AX}||ID_X||N2_A)$ and k milliseconds to compare the computed $MAC'(K_{SA}, K_{AX}||ID_X||N2_A)$ with the received $MAC(K_{SA}, K_{AX}||ID_X||N2_A)$. Thus it may need $j*k*n$ milliseconds at most to confirm the pairwise key K_{AX} is shared with some neighbor node ID_X.

Similarly, when the server S unicasts a response message M_5 to node B, B must verify the authenticity of pairwise session key by decrypting $\{K_{YB}\}_{K_{SB}}$, where Y = 1, 2, 3, …, m and m is the number of key establishment requests of B that are received to establish a shared pairwise key with B. If the shared pairwise key K_{YB} is revealed, B still does not know which neighbor node did B share with. Therefore B may compute m times $MAC'(K_{SB}, K_{YB}||ID_Y||ID_B)$ at most and compares them with some neighbor node. Suppose the node B takes j milliseconds to compute one $MAC'(K_{SB}, K_{YB}||ID_Y||ID_B)$ and k milliseconds to compare the computed $MAC'(K_{SB}, K_{YB}||ID_Y||ID_B)$ with the received $MAC(K_{SB}, K_{YB}||ID_Y||ID_B)$. Thus it may need $j*k*m$ milliseconds at most to confirm the pairwise key K_{YB} is shared with some neighbor node ID_Y. Due to the node of IoT network has constraints on resources such as energy and memory, Nasiraee-Mohasefi's scheme is vulnerable against resource depletion attack on power consumption.

4 The Proposed Scheme

This section proposes a simple improvement on Nasiraee-Mohasefi's scheme, which not only keeps the merits of original scheme but also resists the weaknesses described in previous section. The details of the proposed scheme are described in the following subsections.

4.1 Security Improvement

Considering the insecurity of a pseudo random function $f(.)$ as mentioned in Section 3.1, an attacker C only needs to use the compromised pseudo random function and eavesdropped messages to compute any shared pairwise session key $K_{AX} = f(ID_A||ID_B||N2_A)$. The reason for this attack is because there is no binding between nodes' secret keys and this flaw damages the security of entire IoT system. Therefore, we integrated the secret key K_{SX} to prevent above-mentioned attacks in the proposed scheme. For a secret key K_{SX}, it is a symmetric key known only to node X and server S. If other IoT nodes illegally got the pseudo random function $f(.)$, they are still unable to compute shared pairwise key K_{AB} between node A and node B, because they do not have secret keys K_{SA} and K_{SB}. The details of the proposed scheme are briefly described as follows and Figure 3 shows the flow of the messages in the proposed scheme.

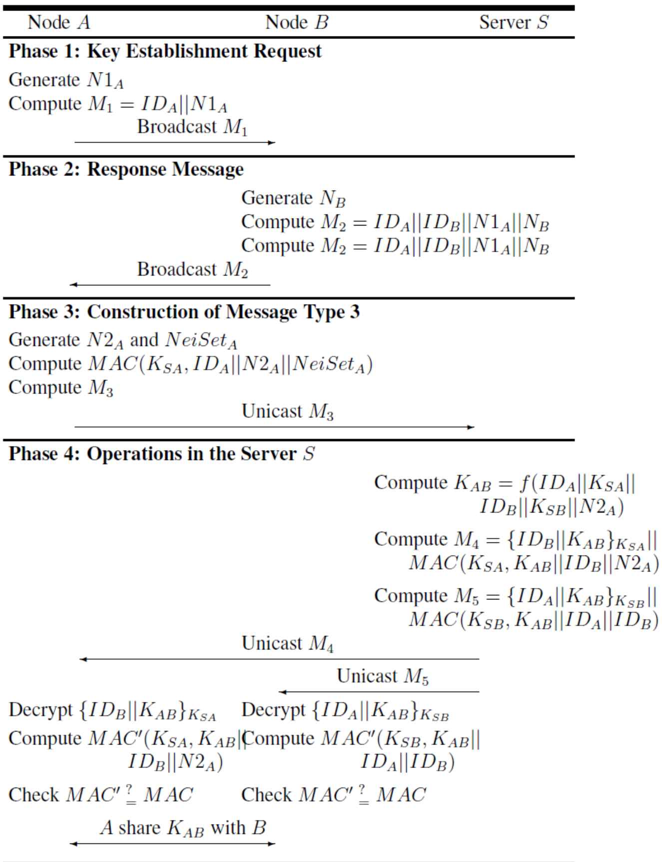

Figure 3. Flow of messages in the proposed scheme

Phase 1: Key establishment request. In this phase, the executed steps are the same as Nasiraee-Mohasefi's scheme.
Phase 2: Response message. In this phase, the executed steps are the same as Nasiraee-Mohasefi's scheme.
Phase 3: Construction of message type 3. In this phase, the executed steps are the same as Nasiraee-Mohasefi's scheme.
Phase 4: Operations in the server *S*. After receiving M_3 from node *A*, the server *S* checks replay attacks on M_3 by $N2_A$. In fact, the server *S* generates messages as many as the number of interested nodes. For simplicity, we have only mentioned the node *B*. *S* establishes a pairwise session key K_{AB} shared between *A* and *B* by computing $K_{AB} = f(ID_A||K_{SA}||ID_B||K_{SB}||N2_A)$. Note that K_{SA} and K_{SB} are integrated into the pseudo random function. After generating K_{AB}, messages M_4 and M_5 would be constructed as follows:

$$M_4 = \{K_{AB}\}_{K_{SA}}||MAC(K_{SA}, K_{AB}||ID_B||N2_A)$$
$$M_5 = \{K_{AB}\}_{K_{SB}}||MAC(K_{SB}, K_{AB}||ID_A||ID_B)$$

After generating messages M_4 and M_5, server *S* unicasts them to the corresponding node *A* and its neighbor node *B*. After receiving M_4 from *S*, node *A* reveals $(ID_B||K_{SB})$ by using the secret key K_{SA} shared between *A* and *S*. Then, A computes $MAC'(K_{SA}, K_{AB}||ID_B||N2_A)$ and compares it with the received $MAC(K_{SA}, K_{AB}||ID_B||N2_A)$. If computed $MAC'(K_{SA}, K_{AB}||ID_B||N2_A)$ is equal to received $MAC(K_{SA}, K_{AB}||ID_B||N2_A)$, *A* convinces that K_{AB} is generated by server *S* and it will be used for securing future IoT communications between node *A* and node *B*.

On the other hand, after receiving M_5 from *S*, node *B* reveals $(ID_A||K_{AB})$ by using the secret key K_{SB} shared between *B* and *S*. Then, B computes $MAC'(K_{SB}, K_{AB}||ID_A||ID_B)$ and compares it with the received $MAC(K_{SB}, K_{AB}||ID_A||ID_B)$. If computed $MAC'(K_{SB}, K_{AB}||ID_A||ID_B)$ is equal to received $MAC(K_{SB}, K_{AB}||ID_A||ID_B)$, *B* convinces that K_{AB} is generated by server *S* and it will be used for securing future IoT communications between node *A* and node *B*.

As mentioned in Section 3.1, the insecurity problem of a pseudo random function is an inherent limitation of three party key establishment scheme. We found that best solution is to integrate some secret values into key generation procedure and we assume that an attacker *C* eavesdrops all the transmission messages (M_1, M_2, M_3) between node *A* and node *B* and makes an effort to obtain a pseudo random function *f*(.). To derive the pairwise session key $K_{AB} = f(ID_A||K_{SA}||ID_B||K_{SB}||N2_A)$, *C* must collect the secret keys (K_{SA}, K_{SB}) at the same time. In fact, *C* is unable to draw all the pairwise session keys because the security of a session key depends on two nodes' secret keys and the proposed scheme can resist the session key disclosure attacks.

4.2 Efficiency Improvement

Considering the nature of low efficiency on Nasiraee-Mohasefi's scheme as mentioned in Section 3.2, every node may compute *n* times *MAC'* and compare them with all the received *MAC'*. Since all received messages are *n*, the time complexity of their scheme is thus O(*n*). It may become infeasible for resource-constrained IoT nodes to authenticate the response results in phase 4 of their scheme. In order to enhance the efficiency of Nasiraee-Mohasefi's scheme, we integrated the node identifier ID_X into Message 4 and Message 5. Afterwards, node *X* will reveal the identifier and know which neighbor node did *X* share with. So the IoT node only needs to compute *MAC'* once in every session and the time complexity of the proposed scheme is O(1). Finally, the proposed scheme is more efficient than Nasiraee-Mohasefi's scheme, which could greatly decrease power consumption for IoT nodes and it is well-suited to adoption in resource-constrained IoT devices.

5 Security Proof of the Proposed Scheme

In this section, we use the BAN logic [2] to analyze the security of the session key between node *A* and node *B*. Some notations used in BAN logic analysis are described as follows:

- $A \mid\equiv X$: It means that *A* believes the formula *X* is true.
- $A \triangleleft X$: It means that *A* sees the formula *X*.
- $A \mid\Rightarrow X$: It means that *A* has complete control over the formula *X*.
- $A \mid\sim X$: It means that *A* has once said the formula *X*.
- #(*X*): It means that *X* is fresh. The formula *X* has not been used before or *X* is a nonce.
- $A \overset{K}{\leftrightarrow} B$: It means that principals *A* and *B* may use the shared key *K* to communicate. Note that *K* will never be discovered by any principals except *A* and *B*.
- $(X)_Y$: It means that formula *X* is combined with a secret parameter *Y*.
- $\{X\}_K$: It means that formula *X* is encrypted by key *K*.

$\frac{Rule1}{Rule2}$ -: It can infer *Rule* 2 from *Rule* 1. For example, $\frac{A \text{ creates random } X}{A \mid\equiv \#(X)}$ means that principal *A* creates *X*, so *A* believes *X* is fresh.

- *SK*: A pairwise session key established in each session.

According to the analytic procedures of BAN logic, two nodes *A* and *B* cooperatively run the proposed scheme with the help of the server *S* and we list the verification goals of our protocol as follows:

Goal 1. $A \mid\equiv A \xleftrightarrow{SK} B$

Goal 2. $B \mid\equiv A \xleftrightarrow{SK} B$

Goal 3. $S \mid\equiv A \xleftrightarrow{SK} B$

Next, we use BAN logic to transform our scheme, illustrated in Figure 3 into the idealized form. The scheme generic types are shown in the following:

Message 1. $A \rightarrow B$: ID_A, $N1_A$

Message 2. $B \rightarrow A$: ID_A, ID_B, $N1_A$, N_B

Message 3. $A \rightarrow S$: ID_A, $N2_A$, $NeiSet_A$, $MAC(K_{SA}, ID_A, N2_A, NeiSet_A)$

Message 4. $S \rightarrow A$: $\{ID_B, SK\}_{K_{SA}}$, $MAC(K_{SA}, SK, ID_B, N2_A)$

Message 5. $S \rightarrow B$: $\{ID_A, SK\}_{K_{SB}}$, $MAC(K_{SB}, SK, ID_A, ID_B)$

Idealize form of the proposed protocol:

Message 1. $A \rightarrow B$: ID_A, $N1_A$

Message 2. $B \rightarrow A$: ID_A, ID_B, $N1_A$, N_B

Message 3. $A \rightarrow S$: ID_A, $N2_A$, $NeiSet_A$, $(ID_A, N2_A, NeiSet_A)_{K_{SA}}$

Message 4. $S \rightarrow A$: $\{ID_B, SK\}_{K_{SA}}$, $(SK, ID_B, N2_A)_{K_{SA}}$

Message 5. $S \rightarrow B$: $\{ID_A, SK\}_{K_{SB}}$, $(SK, ID_A, ID_B)_{K_{SB}}$

Session key. $SK = f(ID_A, K_{SA}, ID_B, K_{SB}, N2_A)$

To analyze the proposed scheme, the following assumptions are also required:

(A.1): $A \mid\equiv \#(N1_A)$

(A.2): $A \mid\equiv \#(N2_A)$

(A.3): $B \mid\equiv \#(N_B)$

(A.4): $A \mid\equiv (A \xleftrightarrow{K_{SA}} S)$

(A.5): $B \mid\equiv (B \xleftrightarrow{K_{SB}} S)$

(A.6): $A \mid\equiv B \mid\equiv (A \xleftrightarrow{K_{SA}} S)$

(A.7): $B \mid\equiv A \mid\equiv (B \xleftrightarrow{K_{SB}} S)$

(A.8): $A \mid\equiv B \triangleleft (A \xleftrightarrow{SK} B)$

(A.9): $B \mid\equiv A \triangleleft (A \xleftrightarrow{SK} B)$

Based on the above-mentioned assumptions, the preliminary procedures of BAN logic are well prepared and we show the main steps of the verification proof as follows:

According to the Message 1, we could obtain:

(V.1): $B \triangleleft N1_A$

According to the Message 2, we could obtain:

(V.2): $A \triangleleft N1_A, N_B$

According to the Message 3, we could obtain:

(V.3): $A \triangleleft ID_A, N2_A, NeiSet_A, (ID_A, N2_A, NeiSet_A)_{K_{SA}}$

According to the assumption **(A.4)**, we apply the message meaning rule to obtain:

(V.4): $S \mid\equiv A \mid\sim N2_A$

According to the assumption **(A.2)** and **(V.4)**, we apply the freshness conjuncatenation rule to obtain:

(V.5): $S\ \#(N2_A, NeiSet_A)_{K_{SA}}$

According to **(V.4)** and **(V.5)**, we apply the nonce verification rule to obtain:

(V.6): $S \mid\equiv A \mid\equiv (N2_A, NeiSet_A)_{K_{SA}}$

According to **(A.4)** and **(V.6)**, we apply the jurisdiction rule to obtain:

(V.7): $S \mid\equiv N2_A$

According to $SK = f(ID_A, K_{SA}, ID_B, K_{SB}, N2_A)$, **(V.7)**, and **(A.5)**, we could obtain:

(V.8): $S \mid\equiv A \xleftrightarrow{SK} B$ (Goal 3.)

According to the Message 4, we could obtain:

(V.9): $A \triangleleft \{ID_B, SK\}_{K_{SA}}, (SK, ID_B, N2_A)_{K_{SA}}$

According to the assumption **(A.4)**, we apply the message meaning rule to obtain:

(V.10): $A \mid\equiv S \mid\sim N2_A$

According to the assumption **(A.2)** and **(V.10)**, we apply the freshness conjuncatenation rule to obtain:

(V.11): $A\ \#(SK, ID_B, N2_A)_{K_{SA}}$

According to **(V.10)** and **(V.11)**, we apply the nonce verification rule to obtain:

(V.12): $A \mid\equiv B \mid\equiv (SK, ID_B, N2_A)_{K_{SA}}$

According to **(A.4)** and **(V.12)**, we apply the jurisdiction rule to obtain:

(V.13): $A \mid\equiv (SK, ID_B, N2_A)_{K_{SA}}$

According to $SK = f(ID_A, K_{SA}, ID_B, K_{SB}, N2_A)$, **(V.13)**, and **(A.5)**, we could obtain:

(V.14): $A \mid\equiv A \xleftrightarrow{SK} B$ (Goal 1.)

According to the Message 5, we could obtain:

(V.9): $B \triangleleft \{ID_A, SK\}_{K_{SB}}, (SK, ID_A, ID_B)_{K_{SB}}$

According to the assumption **(A.5)**, we apply the message meaning rule to obtain:

(V.16): $B \mid\equiv S \mid\sim N2_A$

According to the assumption **(A.2)** and **(V.16)**, we apply the freshness conjuncatenation rule to obtain:

(V.17): $B\ \#(SK, ID_A, ID_B)_{K_{SB}}$

According to **(V.16)** and **(V.17)**, we apply the nonce verification rule to obtain:

(V.18): $B \mid\equiv A \mid\equiv (SK, ID_A, ID_B)_{K_{SB}}$

According to **(A.5)** and **(V.18)**, we apply the jurisdiction rule to obtain:

(V.19): $B \mid\equiv (SK, ID_A, ID_B)_{K_{SB}}$

According to $SK = f(ID_A, K_{SA}, ID_B, K_{SB}, N2_A)$, **(V.19)**, and **(A.4)**, we could obtain:

(V.20): $B \mid\equiv A \xleftrightarrow{SK} B$ (Goal 2.)

Finally, inferring from formulas **V.8**, **V.14** and **V.20**, we have proven the proposed scheme achieves the verification goals as well as establishes a pairwise session key *SK* between node *A* and node *B*.

6 Functionality Analysis

In this section, we compare our proposed scheme with previous three party authentication and key establishment schemes [26, 28] in two aspects: one is the security properties and the other is efficiency. For convenience to evaluate the functional features, we define some notations as follows.

-*F*1: Provision of key establishment.

-*F*2: Provision of formal security proof.

-*F*3: Prevention of synchronized clock attack.

-*F*4: Prevention of Denial-of-Service attack.

-*F*5: Prevention of session key disclosure attack.

-*F*6: Efficiency of node-to-node authentication.

Table 2 shows the comparisons of the proposed scheme with related schemes in terms of security properties. With respect to the security properties, while Perrig et al.'s scheme is vulnerable to DoS attack, Nasiraee-Mohasefi's scheme is resistant to the attack. Similarly, Perrig et al.'s scheme and Nasiraee-Mohasefi's scheme have low efficiency problem during node-to-node authentication. The reason is that Perrig et al.'s scheme has the same problem with Nasiraee-Mohasefi's scheme while a new node A received the response message $\{K_{AB}\}_{K_{SA}}$, $MAC(K_{AB}||N_A||ID_B)$. Moreover, the security of Perrig et al.'s scheme and Nasiraee-Mohasefi's scheme were not proved in a formal model, while our proposed scheme not only satisfies all the security attributes but also provides the rigorous proof of the security. From an implementation point of view, our scheme requires less computational power and achieves more security criteria compared with related schemes and these features make our solution quite suitable to resource-constrained environments such a Internet of Thing environments and the Internet-enabled sensor networks.

Table 2. Functionality comparisons of our proposed scheme with previous three party authentication schemes for IESN

Scheme → Features ↓	Perrig et al. [28]	Nasiraee and Mohasefi [26]	The proposed scheme
$F1$	YES	YES	YES
$F2$	NO	NO	YES
$F3$	YES	YES	YES
$F4$	NO	YES	YES
$F5$	NO	NO	YES
$F6$	NO	NO	YES

7 Conclusions

This paper proposes a new and improved node authentication and key establishment scheme for the Internet of Things environment and is based on the recently proposed novel scheme of Nasiraee-Mohasefi's scheme. During a cryptanalysis of Nasiraee-Mohasefi's scheme, we have demonstrated that their scheme has low efficiency problem during authentication phase. Furthermore, we found that the attacker once has stolen the server S's pseudo random function $f(.)$, and then can perform a session key disclosure attack in Nasiraee-Mohasefi's scheme.

Our proposed scheme tackles and eliminates all weaknesses of Nasiraee-Mohasefi's scheme while preserving the novel approach and all the security and functionality requirements. Moreover, we have also conducted a BAN logic analysis and the security proof shows that our scheme provides a high security level and thus is safe against the most common attacks for the Internet of Things environment.

Acknowledgements

The authors would like to thank the anonymous referees and associate/guest editor for their valuable suggestions and comments. In addition, this paper was supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract no.: MOST 104-2221-E-165-004 and MOST 104-3114-C-165-001-ES.

References

[1] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A Survey, *Computer Networks*, Vol. 54, No. 15, pp. 2787-2805, October, 2010.

[2] M. Burrows, M. Abadi, R. Needham, A Logic of Authentication, *ACM Transactions on Computer Systems*,Vol. 8, No. 1, pp. 18-36, February, 1990.

[3] D. Banerjee, B. Dong, M. Taghizadeh, S. Biswas, Privacy-preserving Channel Access for Internet of Things, *IEEE Internet of Things Journal*, Vol. 1, No. 5, pp. 430-445, October, 2014.

[4] S. K. Bhoi, P. M. Khilar, SIR: A Secure and Intelligent Routing Protocol for Vehicular Ad Hoc Networks, *IET Networks*, Vol. 4, No. 3, pp. 185-194, May, 2015.

[5] T. H. Feng, W. T. Li, M. S. Hwang, A False Data Report Filtering Scheme in Wireless Sensor Networks: A Survey, *International Journal of Network Security*, Vol. 17, No. 3, pp. 229-236, May, 2015.

[6] P. Guo, J. Wang, B. Li, S. Lee, A Variable Threshold-value Authentication Architecture for Wireless Mesh Networks, *Journal of Internet Technology*, Vol. 15, No. 6, pp. 929-936, June, 2014.

[7] D. He, J. Chen, J. Hu, Improvement on a Smart Card Based Password Authentication Scheme, *Journal of Internet Technology*, Vol. 13, No. 3, pp. 405-410, May, 2012.

[8] D. He, W. Zhao, S. Wu, Security Analysis of A Dynamic ID-based authentication Scheme for Multi-server Environment Using Smart Cards, *International Journal of Network Security*, Vol. 15, No. 5, pp. 350-356, September, 2013.

[9] D. He, N. Kumar, 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, November, 2015.

[10] D. He, S. Zeadally, Authentication Protocol for Ambient Assisted Living System, *IEEE Communications Magazine*, Vol. 35, No. 1, pp. 71-77, January, 2015.

[11] D. He, N. Kumar, J. Chen, Robust Anonymous Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks, *Multimedia Systems*, Vol. 21, No. 1, pp. 49-60, February, 2015.

[12] D. He, D. Wang, Robust biometrics-based authentication Scheme for Multi-server Environment, *IEEE Systems Journal*, Vol. 9, No. 3, pp. 816-823, September, 2015.

[13] M. T. I. ul Huque, K. S. Munasinghe, A. Jamalipour, Body Node Coordinator Placement Algorithms for Wireless Body Area Networks, *IEEE Internet of Things Journal*, Vol. 2, No. 1, pp. 94-102, September, 2015.

[14] J. Kohl, C. Neuman, *The Kerberos Network Authentication*

Service (V5), Digital Equipment Corporation, 1993.

[15] C. C. Lee, Y. M. Lai, Toward a Secure Batch Verification with Group Testing for VANET, *Wireless Networks*, Vol. 19, No. 6, pp. 1441-1449, August, 2013.

[16] C. C. Lee, C. T. Chen, C. T. Li, P. H. Wu, A Practical RFID Authentication Mechanism for Digital Television, *Telecommunication Systemss*, Vo. 57, No. 3, pp. 239-246, November, 2014.

[17] C. T. Li, M. S. Hwang, Y. P. Chu, A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular ad Hoc Networks, *Computer Communications*, Vol. 31, No. 12, pp. 2803-2814, July, 2008.

[18] C. T. Li, M. S. Hwang, An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards, *Journal of Network and Computer Applications*, Vol. 33, No. 1, pp. 1-5, January, 2010.

[19] C. T. Li, M. S. Hwang, A Lightweight Anonymous Routing Protocol without Public Key En/decryptions for Wireless Ad Hoc Networks, *Information Sciences*, Vol. 181, No. 23, pp. 5333-5347, December, 2011.

[20] C. T. Li, C. Y. Weng, C. C. Lee, An Advanced Temporal Credential-based Security Scheme with Mutual Authentication and Key Agreement for Wireless Sensor Networks, *Sensors*, Vol. 13, No. 8, pp. 9589-9603, July, 2013.

[21] C. T. Li, C. Y. Weng, C. C. Lee, A Secure RFID Tag Authentication Protocol with Privacy Preserving in Telecare Medicine Information Systems, *Journal of Medical Systems*, Vol. 39, No. 8, Article 77, pp. 1-8, August, 2015.

[22] C. T. Li, C. C. Lee, C. Y. Weng, An Extended Chaotic Maps Based Keyword Search Scheme Over Encrypted Data Resist Outside and Inside Keyword Guessing Attacks in Cloud Storage Services, *Nonlinear Dynamics*, Vol. 80, No. 3, pp. 1601-1611, May, 2015.

[23] C. T. Li, C. C. Lee, C. Y. Weng, A Dynamic Identity Based User Authentication Scheme for Remote Login Systems, *Security and Communication Networks*, Vol. 8, No. 18, pp. 3372-3382, December, 2015.

[24] C. T. Li, C. C. Lee, C. Y. Weng, A Secure Dynamic Identity Based Authentication Protocol with Smart Cards for Multi-server Architecture, *Journal of Information Science and Engineering*, Vol. 31, No. 6, pp. 1975-1992, November, 2015.

[25] C. T. Li, C. C. Lee, C. Y. Weng, A Chaotic Maps Based Key Agreement and User Anonymity Protocol without Using Smart Cards and Symmetric Key En/decryptions, *Journal of Internet Technology*, Vol. 99, No. 99, pp. 91-99, May, 2015.

[26] H. Nasiraee, J. B. Mohasefi, A New Three Party Key Establishment Scheme: Applicable for Internet-enabled Sensor Networks, *Computers & Electrical Engineering*, Vol. 44, pp. 172-183, May, 2015.

[27] K. T. Nguyen, M. Laurent, N. Oualha, Survey on Secure Communication Protocols for the Internet of Things, *Ad Hoc Networks*, Vol. 32, pp. 17-31, February, 2015.

[28] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, D. E. Culler, SPINS: Security Protocols for Sensor Networks, *Wireless Networks*, Vol. 8, No. 5, pp. 521-534, September, 2002.

[29] R. Ramasamy, A. P. Muniyandi, An efficient Password Authentication Scheme for Smart Card, *International Journal of Network Security*, Vol. 14, No. 3, pp. 180-186, May, 2012.

[30] Y. Ren, J. Shen, J. Wang, J. Han, S. Lee, Mutual Verifiable Provable Data Auditing in Public Cloud Storage, *Journal of Internet Technology*, Vol. 16, No. 2, pp. 317-324, March, 2015.

[31] H. Krawczyk, M. Bellare, R. Canetti, *RFC 2014-HMAC, Keyed-hashing for Message Authentication*, http://www.ietf.org/rfc/rfc2014.txt.

[32] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key Management Systems for Sensor Networks in the Context of the internet of things, *Computers & Electrical Engineering*, Vol. 37, No. 2, pp. 147-159, March, 2011.

[33] R. Roman, J. Zhou, J. Lopez, On the Features and Challenges of Security and Privacy in Distributed Internet of Things, *Computer Networks*, Vol. 57, No. 10, pp. 2266-2279, July, 2013.

[34] J. Shen, H. Tan, J. Wang, S. Lee, A Novel Routing Protocol Providing Good Transmission Reliability in Underwater Sensor Networks, *Journal of Internet Technology*, Vol. 16, No. 1, pp. 171-178, January, 2015.

[35] L. K. Sye, S. S. Kumar, H. Tschofenig, Securing the Internet of Things: A Standardization Perspective, *IEEE Internet of Things Journal*, Vol. 1, No. 3, pp. 265-275, June, 2014.

[36] M. Turkanović, B. Brumen, 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, September, 2014.

[37] Y. Wang, H. Zhong, Y. Xu, J. Cui, ECPB: Efficient Conditional Privacy-preserving Authentication Scheme Supporting Batch Verification for VANETs, *International Journal of Network Security*, Vol. 18, No. 2, pp. 374-382, March, 2016.

[38] D. Xu, Z. Wu, Z. Wu, Q. Zhang, L. Qin, J. Zhou, Internet of Things: Hotspot-based Discovery Service Architecture with Security Mechanism, *International Journal of Network Security*, Vol. 17, No. 2, pp. 208-216, March, 2015.

[39] Z. Yan, P. Zhang, A. V. Vasilakos, A Survey on Trust Management for Internet of Things, *Journal of Network and Computer Applications*, Vol. 42, pp. 120-134, June, 2014.

[40] S. Zeng, Y. Huang, X. Liu, Privacy-preserving Communication for VANETs with Conditionally Anonymous Ring Signature, *International Journal of Network Security*, Vol. 17, No. 2, pp. 135-141, March, 2015.

[41] J. Zhou, Z. Cao, X. Dong, N. Xiong, A. V. Vasilakos, 4S: A Secure and Privacy-preserving Key Management Scheme for Cloud-assisted Wireless Body Area Network in M-healthcare Social Networks, *Information Sciences*, Vol. 314, pp. 255-276, September, 2015.

Biographies

Chun-Ta Li received the Ph.D. degree in Computer Science and Engineering from National Chung Hsing University, Taiwan, in 2008. He is currently an Associate Professor with the Department of Information Management at Tainan University of Technology, Taiwan. Dr. Li is currently an editorial board member of International Journal of Network Security and he has published more than 60 papers in International Journals.

Cheng-Chi Lee received the Ph.D. degree in Computer Science from National Chung Hsing University, Taiwan, in 2007. He is currently an Associate Professor with the Department of Library and Information Science at Fu Jen Catholic University, Taiwan. Dr. Lee is currently as an editorial board member of International Journal of Network Security and Journal of Computer Science.

Chi-Yao Weng received the Ph.D. degree in Computer Science from National Tsing Hua University, Taiwan, in 2011. He is currently an Assistant Professor with the Department of Computer Science, National Pingtung University, Taiwan. His research interests include the application of cloud computing, mobile computing, and image processing.