Untraceable and Unclonable Sensor Movement in the Distributed IoT Environment

This paper was downloaded from TechRxiv (<https://www.techrxiv.org>).

LICENSE

CC BY 4.0

SUBMISSION DATE / POSTED DATE

18-07-2021 / 23-07-2021

CITATION

Nurkifli, E Haodudin (2021): Untraceable and Unclonable Sensor Movement in the Distributed IoT Environment. TechRxiv. Preprint. <https://doi.org/10.36227/techrxiv.15000576.v1>

DOI

[10.36227/techrxiv.15000576.v1](https://doi.org/10.36227/techrxiv.15000576.v1)

Untraceable and Unclonable Sensor Movement in the Distributed IoT Environment

E Haodudin Nurkifli

Abstract—This disruptive era has a significant impact on the developing technologies in human beings, such as Internet of Things (IoT). IoT allows people and devices to transmit their data, hence intelligent environments, such as intelligent healthcare system, smart transportation, smart city, etc, are invented. Unfortunately, the wireless-based communication used by IoT opens an adversary to eavesdrop, delete, and alter the data transmitted to each device. In additional, the adversary can perform severe attacks, such as cloning, impersonation, and others. On the other hand, IoT opens a new challenge for achieving the security properties in preserving privacy in untraceable and unclonable device movement. This paper proposed the unclonable and untraceable sensor movement in the distributed IoT environments to resolve the aforementioned problems. The informally and formally analyses were used to ensure that our proposal has achieved security features and withstood from various attacks. Later, a comparison with the related protocols in the computational complexity will make our proposed protocol suitable for the IoT environment.

Index Terms—Internet of Thing, Unclonable, Untraceable, Sensor Movement, Distributed IoT, Attacks.

I. INTRODUCTION

THE distributed IoT environment is an IoT environment consisting of several WSNs; connectivity between WSN and IoT device which can provide remote access and heterogeneous device communication. Several companies have utilized the distributed IoT environments, such as [1] IBM with Smart Planet, which utilizes a sensor as a primary component applied in a smart water management system and smart city. The other project is the HP lab with Central Nervous System for the Earth (CeNSE) by utilizing a sensor as a primary component.

On the other hand, by utilizing 6LoWPAN, it can integrate the components of WSN, such as sensor with web services of SOAP and REST [2], [3], and the other communication services, such as WhatsApp, Line, email, blogs, etc. [4], [5]. However, many challenges must be carefully considered. One of the challenges is related to the security and privacy problem. For example, sensor movement in the distributed IoT-based healthcare system -, in which the patients with the body sensor network want to move from one room to the other room or from one hospital building to the others for treatments by keeping the patients' privacy. While the patients' body sensor can prove their legitimacy, their movements should remain secret for the security reasons.

Several security features must be fulfilled to securely

provide WSN as part of the IoT environment [6]. However, this paper focuses on untraceable and unclonable sensor movement. This proposal also considers achieving the standards of security features, such as mutual authentication, perfect forward and backward secrecy, and withstanding from various kinds of attacks including reply, DoS, and other attacks. Moreover, this paper also uses lightweight cryptography, such as XOR-operation and One-way-hash-function. In addition, PUF is used to achieve a non-cloning device.

This paper is further organized as follows. Section II presents the proposal details, Section III discusses informal analysis. Section IV explains the performance and comparison analysis. Section V, VI, and VII respectively discuss the formal analysis using BAN Logic, ROR model, and Scyther tool. Finally, Section VIII draws the conclusions.

A. Related work and contributions

Several researchers have proposed authentication protocol in the distributed IoT environment, such as Roman et al. [7], discussing the security challenges, the privacy of network entity, untraceability, authentication, and access control. In [7], the sensor can move from one Cluster to the other Cluster and move from one network to the others. [8] proposed the authentication protocol in WSNs for the distributed IoT using the master key. Further research proposed by [9] discussed the authentication protocol in WSN application using ticket. Unfortunately, most of those researchers only proposed the user authentication, and do not offer mutual authentication and key establishment between device and server, in which it is imperative for the communication security [10].

In [11] and [12] proposed the broadcast authentication in

Manuscript submitted July 16, 2021; This work was support by the National Science Council of Taiwan under Contract No. MOST 109-2221-E-006-168-; No. MOST 108-2221-E-006-107.

The author is with the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan 701, Taiwan, Universitas Singaperbangsa Karawang, Karawang, Indonesia (e-mail: dudink95@gmail.com, dudi.nurkifli@staff.unsika.ac.id).

the WSN environment. [13] proposed the secure communication using Datagram Transport Layer Security (DTLS). However, [14] found that [13] DTLS based on the secure version of Constrained Application Protocol (CoAP) is undependable in an IoT environment. [15] proposed two-manner authentication protocol in IoT. However, their scheme [15] has a high computational burden since using X.509 certificates and public-key cryptosystems known as RSA, yet their scheme is unsuitable for application in sensor nodes with the limited resources. The other researchers [16]–[19] proposed the authentication protocols using Elliptic Curve Digital Signature (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH). However, [16]–[19] also have a height computational burden similar to [15]; It can be said [16]–[19] are also not suitable to apply in sensor nodes. In addition, the aforementioned authentication protocol did not achieve the security features, such as anonymity and untraceability [10].

Gope and Hwang [10] proposed the untraceable sensor movement in the distributed IoT environment. However, based on our investigation, their scheme fails to achieve the untraceability. The attacker has the ability to intercept all messages in a public channel, capture the sensor, and obtain the data from the sensor's memory including the secret key. The attacker then continuously acquires a set of the sequence numbers $\{Tr_{seq}, Tr_{seq} + 1, Tr_{seq} + 2, \dots\}$. Based on the collected message, the attacker will figure out two messages from a similar sensor. In addition, the attacker can impersonate the sensor based on its owned key. On the other hand, most of the previous authentication protocols including the scheme of Gope and Hwang, cannot guarantee the unclonable devices. Therefore, the majority of previous schemes cannot withstand from the cloning attacks.

This article endeavors to resolve the problems which cannot be achieved by the previous scheme [15], [19], and [10]. The contributions of this proposal are explained as follows:

1. Designing a new protocol using PUF, with the main contributions of both untraceable and unclonable sensors.
2. Achieving the mutual authentication, perfect forward and backward secrecy.
3. The proposed authentication protocol can withstand from various kinds of attacks, such as to reply, DoS, impersonation, and cloning attack.
4. Analyzing formally using BAN Logic to ensure that the

II. PROPOSED SCHEME

This section presents the proposed authentication protocol starting from System architecture, Assumptions, Notation, Registration phase between Cluster Head and Home IoT Server, Registration between Sensor and Home IoT Server, Authentication in inter-cluster movement phase, authentication in inter-network movement phase, Updated challenge-response phase. (See figure 2 and 3). For convenience, notations are used in Table 1 throughout the authentication protocol.

A. System Architecture

This subsection presents a brief description of IoT distributor environment.

In Fig 1, the system structure adopts the authentication

authentication protocol has achieved the secure mutual authentication. In addition, analyzing formally using the RoR model and Scyther tool ensures that that the proposed protocol withstands from various attacks.

5. A comparison of security features and computational complexity ensures that the proposal is secure and has low computational complexity.

B. Preliminaries

This subsection briefly presents the preliminary background of PUF

Physically Unclonable Function (PUF)

PUF is a unique property of circuit mapping the Challenge C to Response R in a chip manufacturing process [20]. Formally, C is inputted into PUF to produce R where $R = \text{PUF}(C)$. Significantly, PUFs are hard to clone [21]. PUF is divided into two types: non-ideal and ideal PUF. Non-ideal PUF may produce a different response with the similar input Challenge C into PUF due to the temperature. The fuzzy extractor is used to ensure the stability of PUF output [22], [23]; however, a fuzzy extractor increases the computational overhead. Meanwhile, ideal PUF may produce a similar response with similar challenges inputted into PUF. Even if the factor of non-stable temperature occurs, in the last few years, researchers have developed an ideal PUF, ensuring 0% Bit-Error Rate [24]–[27]. Therefore, in this paper, the ideal PUF or stable PUF is utilized.

TABLE I
NOTATIONS OF CRYPTOGRAPHIC FUNCTIONS

Notation	Definition
ID_{sh}	Identity of cluster head
ID_{ch}	Identity of Home IoT Server
ID_h	Shared key between cluster head and Home IoT server
K_{ch}	Physically unclonable function of sensor
PUF_s	One-time Pseudonym of sensor to communicate with Home IoT server
PID_{sh}	Challenge-response pairs
(C_s, R_s)	Concatenation operation
$\parallel$	Exclusive-OR operation
$\oplus$	Pseudo identity of synchronization is used if the synchronization loss occurs where $PID_{syn} = \{pid_1, \dots, pid_n\}$
PID_{syn}	Challenge of synchronization is used if the synchronization loss occurs where $C_{syn} = \{c_1, \dots, c_n\}$
C_{syn}	Identity of cluster head

protocol proposed by [10]. For convenience, several terms are introduced, such as Sensor Node (SN), Cluster Head (CH), Home IoT Server (HIO TS), and Cloud Server (CS). SN collects the data from users, CH Forwards data to Home IoT Server; HIO TS is a database to store the data from sensor and CH in each WSN, and CS Managing HIO TS.

Fig. 1. Structure System of the Distributed IoT Environment.

B. Assumptions

Several assumptions are presented as follows.

1. Sensor is equipped with PUF.
2. PUF onboard is in sensor, if attacker attempts to tamper, PUF will be destroyed.
3. Sensor has constrained resources
4. Cluster head and home IoT Server do not have the constrained resources

C. Notations of Cryptographic Functions

This subsection presents the notations of cryptographic functions. In addition, based on the aforementioned assumptions, the sensors are equipped with PUF; hence the scheme uses this facility (See table 1).

D. Registration of Cluster Head via secure channel

In this subsection, registration of cluster head is presented via a secure channel and each step at this phase is as follows:

Step 1: CH selects its identity ID_{ch} and sends ID_{ch} , $RegReq$ to the HIoTTS

Step 2: HIoTTS generates the shared key K_{ch} for CH, and HIoTTS, stores K_{ch} , ID_{ch} , and then sends K_{ch} to CH

Step 3: finally, CH stores K_{ch} , ID_{ch} .

E. Registration of Sensor via a secure channel

In this subsection registration of Sensor Node is presented via a secure channel and each step at this phase is as follows:

Step 1: Sensor sends identity and registration-request ID_s , $RegReq$ to HIoTTS.

Step 2: HIoTTS generates challenge C_s , pseudo-identity PID_{sh} to achieve anonymity of sensor to communicate with Home IoT server, pseudo identities synchronization $PID_{syn} = \{pid_1, pid_2, \dots, pid_n\}$, and challenges for synchronization $C_{syn} = \{c_1, c_2, \dots, c_n\}$, then HIoTTS sends C_s , C_{syn} , PID_{sh} ,

PID_{syn} to SN.

Step 3: SN generates a response $R_s = PUF(C_s)$ and responses for synchronization $R_{syn} = PUF(C_{syn})$ where $R_{syn} = \{r_1, r_2, \dots, r_n\}$ SN stores PID_{sh} , PID_{syn} . SN sends R_s , R_{syn} to HIoTTS.

Step 4: HIoTTS stores C_s , R_s , ID_s , PID_{sh} , PID_{syn} , (C_{syn}, R_{syn})

If synchronization loss occurs, SN replaces PID_{sh} by PID_{syn} , and runs similar to the authentication phase.

F. Authentication in inter-cluster movement phase

This subsection presents the phase of authentication in inter-cluster movement and each step at this phase is as follows:

Step 1: SN generates N_s , computes $V_1 = h(PID_{sh} || N_s || ID_s || ID_h)$, sends $M_1: \{PID_{sh}, N_s, ID_h, V_1\}$ to C-CH

Step 2: After receiving $M_1: \{PID_{sh}, N_s, ID_h, V_1\}$, C-CH generates N_c , computes $N_c^* = N_c \oplus h(K_{ch})$, $V_2 = h(M_1 || K_{ch} || N_c || ID_{ch})$, and sends $M_2: \{ID_{ch}, N_c^*, V_2, M_1\}$ to HIoTTS.

Step 3: After receiving $M_2: \{ID_{ch}, N_c^*, V_2, M_1\}$, HIoTTS checks PID_{sh} , computes $N_c = N_c^* \oplus h(K_{ch})$, verifies V_1 and V_2 , reads (C_s, R_s) , generates N_h , computes $N_h^* = N_h \oplus h(N_s || R_s)$, updates $PID_{sh} = PID_{sh}^{new} \oplus h(ID_s || R_s)$, and computes $V_3 = h(K_{ch} || N_c || ID_{ch})$, $V_4 = h(PID_{sh} || C_s || ID_s || N_h^* || N_h || R_s)$, HIoTTS then sends $M_3: \{PID_{sh}, N_h^*, C_s, V_3, V_4\}$ to C-CH.

Step 4: After receiving $M_3: \{PID_{sh}, N_h^*, C_s, V_3, V_4\}$, C-CH computes and verifies $V_3^* = h(K_{ch} || N_c || ID_{ch}) ? V_3$. C-CH then sends $M_4: \{PID_{sh}, N_h^*, C_s, V_4\}$ to SN.

Step 5: After receiving $M_4: \{PID_{sh}, N_h^*, C_s, V_4\}$, SN computes $R_s = PUF(C_s)$, $N_h = N_h^* \oplus h(N_s || R_s)$, verifies V_4 , and updates $PID_{sh}^{new} = PID_{sh} \oplus h(ID_s || R_s)$.

Fig. 2. Authentication in inter-cluster movement

G. Authentication in inter-network movement phase

This subsection presents the phase of authentication in inter-network movement and each step at this phase is as follows:

SN first sends $M_1: \{PID_{sh}, N_s, ID_h, V_1\}$ to C-CH. SN then moves to other network; C-HloTS is helped by O-HloTS to authentic SN movement, communication between C-HloTS and O-HloTS via the secure channel. The details of these steps are presented as follow:

Step 1: C-CH sends $M_2: \{ID_{ch}, N_c^*, V_2, M_1\}$ to C-HloTS.

Step 2: After receiving $M_2: \{ID_{ch}, N_c^*, V_2, M_1\}$, C-HloTS checks ID_h with its owner identity; if it does not match, C-HloTS then sends $M_1: \{PID_{sh}, N_s, ID_h, V_1\}$ to O-HloTS.

Step 3: After receiving $M_1: \{PID_{sh}, N_s, ID_h, V_1\}$, O-HloTS checks PID_{sh} , verifies V_1 , reads (C_s, R_s) , generates N_h , and computes $N_h^* = N_h \oplus h(N_s || R_s)$, $PID'_{sh} = PID_{sh} \oplus h(ID_s || R_s)$, $V_3 = h(K_{ch} || N_c || ID_{ch})$, $V_4 = h(PID'_{sh} || C_s || ID_s || N_h^* || N_h || R_s)$. O-HloTS then sends $M_3: \{PID'_{sh}, N_h^*, C_s, V_3, V_4\}$ to C-HloTS.

Step 4: After receiving $M_3: \{PID'_{sh}, N_h^*, C_s, V_3, V_4\}$, C-HloTS computes and verifies $V_3^* = h(K_{ch} || N_c || ID_{ch}) ? V_3$, computes

$V_5 = h(M_3 || V_5 || ID_{ch})$, sends $M_4: \{M_3, V_5\}$ to C-CH.

Step 5: After receiving $M_4: \{M_3, V_5\}$, C-CH computes and verifies $V_5^* = h(M_3 || V_5 || ID_{ch}) ? V_5$, C-CH sends $M_3: \{PID'_{sh}, N_h^*, C_s, V_4\}$ to SN.

Step 6: After receiving $M_3: \{PID'_{sh}, N_h^*, C_s, V_4\}$, SN computes $R_s = PUF(C_s)$, $N_h = N_h^* \oplus h(N_s || R_s)$, verifies V_4 , and then computes $PID_{sh}^{new} = PID'_{sh} \oplus h(ID_s || R_s)$.

H. Updated challenge-response phase

This subsection discusses the updated challenge-response.

Step 1: HloTS generates a nonce N_1 , selects challenge-response (C_s, R_s) , and pseudo-identity PID_{sh} . HloTS considers updating the challenge C_s^{new} , encrypts the new challenge using the response $C_s^{new,enc} = C_s^{new} \oplus h(R_s || N_1)$, and computes authentication code $V_1 = h(ID_s || N_1 || R_s || PID_{sh} || C_s^{new,enc} || C_s^{new})$. HloTS then sends to SN.

Step 2: SN generates response $R_s = PUF(C_s)$, decrypts $C_s^{new} = C_s^{new,enc} \oplus h(R_s || N_1)$ to obtain a new challenge C_s^{new} , and verifies V_1 . Sensor generates new response $R_s^{new} =$

Fig. 3. Authentication in inter-network movement

$PUF(C_s^{new})$, computes $N_2 = R_s^{new} \oplus h(R_s)$, $V_2 = h(ID_s || N_1 || R_s || N_2 || R_s^{new})$, updates pseudo-identity $PID_{sh}^{new} = h(ID_{sh} || R_s)$, stores new pseudo-identity PID_{sh}^{new} , and sends N_2, V_2 to HIoT.

Step 3: after receiving N_2, V_2 , HIoT computes $R_s^{new} = N_2 \oplus h(R_s)$ to obtain R_s^{new} , verifies V_2 , and update the pseudo-identity of SN, that is $PID_{sh}^{new} = h(ID_{sh} || R_s)$. Finally, HIoT stores new {challenge, response, pseudo-identity of SN}, that is $C_s^{new}, R_s^{new}, PID_{sh}^{new}$.

III. INFORMAL ANALYSIS AND COMPARISON

This section presents the informal analysis using intuitive reasoning to show that the scheme has achieved the security features. This section also compares the capabilities to withstand from many kinds of attacks with the previous authentication protocols proposed by [15], [19], and [10].

A. Informal Analysis

This subsection presents the details of security feature analysis as follows:

a. Mutual Authentication

All parties identify the identity of other parties by the possession of shared key K_{ch} and private response R_s as well as respectively check nonce N_s, N_h , and N_c to ensure freshness. Therefore, our scheme achieves the mutual authentication.

b. Sensor Anonymity and Untraceability

In our scheme, the sensor uses a one-time pseudonym PID_{sh} to communicate with HIoT. The attacker cannot obtain a real identity, even if the attacker intercepts all messages in a public channel. Therefore, our scheme achieves sensor anonymity and untraceability.

c. Perfect forward and backward secrecy

Even if the attacker steals the sensor and obtains all data from the sensor, intercepts all messages from a public channel. The attacker cannot get both past and future responses. Therefore, this proposed protocol achieves perfect forward and backward secrecy.

d. Resolved synchronization loss problems

If a synchronization loss occurs, the sensor replaces PID_{sh} by pid_1 , IoT Home server replaces C_s by c_1 running the same step with the authentication phase; subsequently, the sensor deletes pid_1 in $PID_{syn} = \{pid_1, pid_2, \dots, pid_n\}$, and k_1 in $K_{syn} = \{k_1, k_2, \dots, k_n\}$. Therefore, our scheme resolves the synchronization loss problem.

B. Attack Analysis

This subsection presents the details of attack analysis as follows:

a. Withstanding from impersonation attack

The attacker cannot reveal a future response even if the attacker steals the sensor; hence, the attacker cannot impersonate the sensor. Therefore, our proposal withstands from impersonation attack.

b. Withstanding from reply attack

In our scheme, a message updates in every session, e.g., M_1 , if attacker intercepts a message in a public channel, e.g., M_1 and resends M_1 , HIoT will be easily detected based on PID_{sh}^{new} , a new nonce.

c. Withstanding from cloning attack

In our scheme, the sensor is equipped with PUF; therefore, our protocol withstands from a cloning attack.

d. Withstanding from DoS attack

Based on the achievement to resolve the synchronization loss, our protocol can withstand from DoS attack.

e. Withstanding from tracking attack

Based on the achievement of the sensor's anonymity and untraceability, therefore, our protocol can withstand from a tracking attack.

C. Comparison

This section presents a comparison between our proposed scheme with the previous protocol authentication offered by [15], [19], and [10] in terms of security features and capability to resist attack. The comparison is presented in the table below:

TABLE II
COMPARISON OF SECURITY FEATURES

Schemes	SF1	SF2	SF3	SF4	SF5
Kothmayr et al. [15]	No	No	No	No	No
Porambage et al.[19]	Yes	No	No	Yes	No
Gope and Hwang [10]	Yes	Yes	No	Yes	No
Our Proposal	Yes	Yes	Yes	Yes	Yes

Where SF: Security Features, SF1: Mutual authentication, SF2: anonymity, SF3: untraceability, SF4: protected impersonation attack, SF5: protected cloning attack

Table 2. shows that the scheme of Kothmayr et al. [15] fails to achieve all security features of SF1-SF5. The scheme of Porambage et al. [19] fails to achieve SF2, SF3, and SF5, but their scheme achieves SF1, SF4. The authentication protocol of Gope and Hwang [10] has the security features of SF1, SF2, and SF4 but does not achieve SF3 and SF5. Only our protocol can achieve all security features (SF1-SF5).

IV. PERFORMANCE ANALYSIS AND COMPARISON

This section presents a comparison between our proposed scheme with the previous authentication protocols proposed by [15], [19], and [10] in terms of computational complexity and execution time of the cryptographic operations. The comparison is presented in the table below:

TABLE III
COMPARISON OF COMPUTATIONAL COMPLEXITY

Schemes	sensor	Cluster Head	HIoT
Kothmayr et al. [15]	N/A	N/A	N/A
Porambage et al.[19]	N/A	N/A	N/A
Gope and Hwang [10]	$4T_h$	$2T_h$	$4T_h$
Our Proposal	$T_{PUF} + 4T_h$	$2T_h$	$3T_h$

Where T_h : Time of one-way hash function, T_{PUF} : Time of PUF process

Table 3 presents the computational complexity of schemes, respectively. Kothmayr et al. [15] and Porambage et al. [19] do not provide computational complexity analysis. In Gope and Hwang [10], the sensor gets the computational complexity $4T_h$, cluster head obtains $2T_h$, and Home IoT Server has the computational complexity $4T_h$. Our scheme has the result of sensor $T_{FE,Rec} + T_{PUF} + 4T_h$, Cluster Head $2T_h$, and Home IoT Server gets $3T_h$.

Computational time based on experimental result is proposed by [10], showing that RSA has the result of 15.91 ms, ECC has the result of 13.22 ms, one-way-has-function has the result of 0.026 ms, PUF has the result of 0.12 ms.

Fig. 4. Diagram of execution time comparison.

The diagram in Fig 4 shows that our protocol has a lower execution time than that of schemes of Kothmayr et al. and Porambage et al.. Hence, our protocol has a low execution time and fulfills the achievement of all security features of SF1-SF5.

V. FORMAL ANALYSIS USING BAN LOGIC

This subsection presents BAN logic as formal analysis to prove the mutual authentication.

This section presents a formal analysis using BAN logic. The following codes will be used throughout the analysis; sensor node (SN), Cluster Head (CH), and Home IoT Server (HIoTS).

A. A brief explanation of BAN Logic

BAN Logic has three objects [28]: participants, encryption keys, and logical formulas. In this paper, the participants are SN, CH, and HIoTS; encryption keys are K_{ch} , R_s , logical formulas as follows. P believes X denoted by $P| \equiv X$, P sees X denoted by $P \triangleright X$, P once said X denoted by $P| \sim X$, P has jurisdiction over X denoted by $P| \Rightarrow X$, X is fresh denoted by $\#(X)$, P and Q may use the shared K to communicate denoted by $P \stackrel{K}{\leftrightarrow} Q$, P processes or is capable of processing, formula X denoted by $P \ni X$, Formula X is encrypted under key K denoted by $\{X\}_K$. In addition, BAN Logic analysis relies on the postulates as follows.

- 1) R1 is the rule of Message-meaning: $\frac{P| \equiv P \leftrightarrow Q, \Delta\{X\}_K}{P| \equiv Q| \sim X}$
- 2) R2 is the rule of Nonce-verification: $\frac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$
- 3) R3 is the rule of Jurisdiction: $\frac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$
- 4) R4 is the rule of Seeing: $\frac{P \Delta(X, Y)}{P \Delta X}$, rule R5: $\frac{P| \equiv P \leftrightarrow Q, P \Delta\{X\}_K}{P \Delta X}$
- 5) R6 is the rule of Freshness: $\frac{P| \equiv \#(X)}{P| \equiv \#(X, Y)}$
- 6) R7 is the rule of Belief: $\frac{P| \equiv (X, Y)}{P| \equiv X}$

B. Proof of Formal analysis on the scheme using BAN Logic

This subsection presents the formal analysis on Authentication in inter-cluster movement phase, starting from the idealized protocol, logical formula, goal, assumptions, and proof protocol analysis.

a. Ideal Protocol

we have created the ideal protocol and omitted the first process,

- Step 2: $CH \rightarrow HIoTS: ID_{ch}, N_c^*, V_2, M_1: \{PID_{sh}, N_s, ID_h, V_1\}$
 Step 3: $HIoTS \rightarrow CH: PID_{sh}', N_h^*, C_s, V_3, V_4$
 Step 4: $CH \rightarrow SN: PID_{sh}', N_h^*, C_s, V_4$

b. Logical formula

This subsection presents the logical formula as follows:

- Step 2: $CH \rightarrow HIoTS: \{ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}\}_{K_{ch}}$
 Step3: $HIoTS \rightarrow$
 $CH: \{\{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3\}_{K_{ch}||N_c||ID_{ch}}$
 Step 4: $CH \rightarrow SN: \{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s$

c. Goal

This subsection presents the goals as follows:

- G1: $CH| \equiv (CH \stackrel{K_{ch}}{\leftrightarrow} HIoTS)$
 G2: $HIoTS| \equiv (CH \stackrel{K_{ch}}{\leftrightarrow} HIoTS)$
 G3: $SN| \equiv (SN \stackrel{R_s}{\leftrightarrow} HIoTS)$
 G4: $HIoTS| \equiv (SN \stackrel{R_s}{\leftrightarrow} HIoTS)$

d. Assumption

This subsection presents the assumptions as follows.

- A1: $HIoTS| \equiv (SN \stackrel{ID_s}{\leftrightarrow} HIoTS)$
 A2: $HIoTS| \equiv \#N_s$
 A3: $HIoTS| \equiv (CH \stackrel{K_{ch}}{\leftrightarrow} HIoTS)$

$$A4: HIoTS| \equiv \#N_c$$

$$A5: CH| \equiv (CH \xleftrightarrow{K_{ch}} HIoTS)$$

$$A6: CH| \equiv \#N_c$$

$$A7: SN| \equiv (SN \xleftrightarrow{R_s} HIoTS)$$

$$A8: SN| \equiv \#N_h$$

$$A9: SN| \equiv \#N_s$$

e. Proof Protocol Analysis using BAN Logic

Proof 1: based on step 2, the message meaning of A1 is obtained as follows.

$$\frac{HIoTS| \equiv (SN \xleftrightarrow{ID_s} HIoTS), \quad HIoTS \triangleleft (\{PID_{sh}, N_s, ID_h\}_{ID_s}), \quad SN \xleftrightarrow{ID_s} HIoTS}{HIoTS| \equiv SN| \sim (PID_{sh}, N_s, ID_h), \quad SN \xleftrightarrow{ID_s} HIoTS}$$

Because HIoTS believes that HIoTS and SN share a private identity, HIoTS sees that $\{PID_{sh}, N_s, ID_h\}_{ID_s}$ is recognized by the identity of sensor ID_s , SN believes that HIoTS once said (PID_{sh}, N_s, ID_h)

Proof 2: using proof 1 and A2, the freshness is obtained as follows.

$$\frac{HIoTS| \equiv \#(N_s)}{HIoTS| \equiv \#(N_s, (PID_{sh}, N_s, ID_h))}$$

Because HIoTS believes that N_s is fresh, HIoTS believes $(N_s, (PID_{sh}, N_s, ID_h))$ are fresh

Proof 3: using proof 2, the nonce-verification is obtained as follows.

$$\frac{HIoTS| \equiv SN| \sim (SN \xleftrightarrow{ID_s} HIoTS, (PID_{sh}, N_s, ID_h)), \quad HIoTS| \equiv \#(N_s)}{HIoTS| \equiv \#(N_s, (PID_{sh}, N_s, ID_h))}$$

Because HIoTS believes that SN once said (PID_{sh}, N_s, ID_h) and HIoTS believes that N_s is fresh, HIoTS believes that the $(N_s, (PID_{sh}, N_s, ID_h))$ are fresh

Proof 4: using proof 3, the belief rules is obtained as follows.

$$\frac{HIoTS| \equiv SN| \sim (N_s, (PID_{sh}, N_s, ID_h)), \quad HIoTS| \equiv \#(N_s)}{HIoTS| \equiv SN| \equiv (N_s, (PID_{sh}, N_s, ID_h))}$$

Because HIoTS believes that SN once said $(N_s, (PID_{sh}, N_s, ID_h))$ and HIoTS believes that N_s is fresh, HIoTS believes that SN believes $(N_s, (PID_{sh}, N_s, ID_h))$

$$\frac{HIoTS| \equiv SN| \equiv (N_s, (PID_{sh}, N_s, ID_h))}{HIoTS| \equiv SN| \equiv (PID_{sh}, N_s, ID_h)} \quad (\text{Goal 4})$$

Because HIoTS believes that SN believes $(N_s, (PID_{sh}, N_s, ID_h))$, HIoTS believe that SN believes (PID_{sh}, N_s, ID_h)

Proof 5: based on step 2, the message meaning of A3 is obtained as follows.

$$\frac{HIoTS| \equiv (CH \xleftrightarrow{K_{ch}} HIoTS), \quad HIoTS \triangleleft (\{ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}\}_{K_{ch}}), \quad CH \xleftrightarrow{K_{ch}} HIoTS}{HIoTS| \equiv CH| \sim (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}), \quad CH \xleftrightarrow{K_{ch}} HIoTS}$$

Because HIoTS believes that CH and HIoTS share key K_{ch} , HIoTS sees that $(\{ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}\}_{K_{ch}})$ is encrypted by K_{ch} , HIoTS believes that CH once said $(ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s})$

Proof 6: using proof 5 and A4, the freshness is obtained as follows.

$$HIoTS| \equiv \#(N_c)$$

$$HIoTS| \equiv \#(N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}))$$

Because HIoTS believes that N_c is fresh, HIoTS believes $(N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}))$ are fresh

Proof 7: using proof 6, the nonce-verification is obtained as follows.

$$\frac{HIoTS| \equiv CH| \sim (CH \xleftrightarrow{K_{ch}} HIoTS, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s})), \quad HIoTS| \equiv \#(N_c)}{HIoTS| \equiv \#(N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}))}$$

Because HIoTS believes that CH once said $(ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s})$ and HIoTS believes that N_c is fresh, HIoTS believes that $(N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}))$ are fresh

Proof 8: using proof 7, the belief rules is obtained as follows.

$$\frac{HIoTS| \equiv CH| \sim (N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s})), \quad HIoTS| \equiv \#(N_c)}{HIoTS| \equiv CH| \equiv (N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}))}$$

Because HIoTS believes that CH once said $(N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}))$ and HIoTS believes that N_c is fresh, the HIoTS believes that CH believes $(N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}))$

$$\frac{HIoTS| \equiv CH| \equiv (N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}))}{HIoTS| \equiv CH| \equiv (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s})} \quad (\text{Goal 2})$$

Because HIoTS believes that CH believes $(N_c, (ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s}))$, HIoTS believe that CH believes $(ID_{ch}, N_c, \{PID_{sh}, N_s, ID_h\}_{ID_s})$

Proof 9: based on step 3, the message meaning of A5 is obtained as follows.

$$\frac{CH| \equiv (CH \xleftrightarrow{K_{ch}} HIoTS), \quad CH \triangleleft (\{ \{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3 \}_{K_{ch}||N_c||ID_{ch}}), \quad CH \xleftrightarrow{K_{ch}} HIoTS}{CH| \equiv HIoTS| \sim (\{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3, CH \xleftrightarrow{K_{ch}} HIoTS)}$$

Because CH believes that CH and HIoTS share key K_{ch} , CH sees that $(\{ \{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3 \}_{K_{ch}||N_c||ID_{ch}})$ is encrypted by K_{ch} , CH believes that HIoTS once said $(\{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3)$

Proof 10: using proof 9 and A6, the freshness is obtained as follows.

$$CH| \equiv \#(N_c)$$

$$CH| \equiv \#(N_c, (\{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3))$$

Because CH believes that N_c is fresh, CH believes $(N_c, (\{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3))$ are fresh

Proof 11: using proof 10, the nonce-verification is obtained as follows.

$$\frac{CH| \equiv HIoTS| \sim (\{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3), \quad CH| \equiv \#(N_c)}{CH| \equiv \#(N_c, (\{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3))}$$

Because CH believes that HIoTS once said $(N_c, (\{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3))$ and CH believes that N_c is fresh, CH believes that $(N_c, (\{PID_{sh}^{new}\}_{ID_s||R_s}, \{N_h\}_{R_s||N_s}, C_s, V_3))$ are fresh

Proof 12: using proof 7, the belief rules is obtained as

follows.

$$\frac{CH \equiv \text{HloTS} \sim (N_c, (\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s, V_3), CH) \equiv \#(N_c)}{CH \equiv \text{HloTS} \equiv (N_c, (\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s, V_3))}$$

Because CH believes that HloTS once said $(N_c, (\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s, V_3))$ and CH believes that N_c is fresh, the CH believes that HloTS believes $(N_c, (\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s, V_3))$

$$\frac{CH \equiv \text{HloTS} \equiv (N_c, (\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s, V_3))}{CH \equiv \text{HloTS} \equiv (\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s, V_3))} \quad (\text{Goal 1})$$

Because CH believes that HloTS believes $(N_c, (\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s, V_3))$, CH believe that HloTS believes $(\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s, V_3))$

Proof 13: based on step 4, the message meaning of A7 is obtained as follows.

$$\frac{SN \equiv (SN \xleftrightarrow{R_s} \text{HloTS}), SN \triangleleft (\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s), SN \xleftrightarrow{R_s} \text{HloTS}}{SN \equiv \text{HloTS} \sim (PID_{sh}^{new}, N_h, C_s), SN \xleftrightarrow{R_s} \text{HloTS}}$$

Because SN believes that SN and HloTS share key R_s based on $R_s = \text{PUF}(C_s)$, SN sees that $(\{PID_{sh}^{new}\}_{ID_s || R_s}, \{N_h\}_{R_s || N_s}, C_s)$ is encrypted by R_s , SN believes that HloTS once said $(PID_{sh}^{new}, N_h, C_s)$

Proof 14: using proof 13, the freshness of A8, and A9 is obtained as follows.

$$\frac{SN \equiv \#(N_s, N_h)}{SN \equiv \#(N_s, N_h, (PID_{sh}^{new}, N_h, C_s))}$$

Because SN believes that N_s, N_h are fresh, SN believes $(N_s, N_h, (PID_{sh}^{new}, N_h, C_s))$ are fresh

Proof 15: using proof 14, the nonce-verification is obtained as follow:

VI. ANALYSIS FORMALLY USING REAL OR RANDOM (ROR) MODEL

In this section, we have also proven the security analysis formally using the ROR model. The analysis results are as follows.

Our ROR model has three participants: Sensor Node (SN_i), Current Cluster Head (CCH_i), and Home IoT server (HloTS) as follows.

- 1) **Participants:** $\pi_{SN_i}^{sn}$, $\pi_{CCH_i}^{cch}$, and $\pi_{\text{HloTS}}^{hiots}$ are the oracles of $sn, cch, hiots$ related to Sensor Node (SN_i), Current Cluster Head (CCH_i), Home IoT server (HloTS)
- 2) **Partnering:** the partnering is achieved if and only if "fulfilling two conditions": 1. Communication between $\pi_{SN_i}^{sn}$ and $\pi_{\text{HloTS}}^{hiots}$ based on communication session-id sid . 2. The uniqueness of all messages transmitted between $\pi_{SN_i}^{sn}$ and $\pi_{\text{HloTS}}^{hiots}$.
- 3) **Freshness:** The freshness is achieved if the adversary cannot divulge the session key SK between $\pi_{SN_i}^{sn}$ and $\pi_{\text{HloTS}}^{hiots}$
- 4) **Adversary:** The adversary $\mathcal{A}$ has capabilities with the Dolev-Yao (DY) adversary model [29], where the adversary can fully control the transmitted message in the public channels. The adversary $\mathcal{A}$ can perform eavesdropping, altering, deleting, and also accessing the queries as follows.

$$\frac{SN \equiv \text{HloTS} \sim (SN \xleftrightarrow{R_s} \text{HloTS}, (PID_{sh}^{new}, N_h, C_s)), SN \equiv \#(N_s, N_h)}{SN \equiv \#(N_s, N_h, (PID_{sh}^{new}, N_h, C_s))}$$

Because SN believes that HloTS once said $(PID_{sh}^{new}, N_h, C_s)$ and SN believes that N_s, N_h are fresh, SN believes that the $(N_s, N_h, (PID_{sh}^{new}, N_h, C_s))$ are fresh

Proof 16: using proof 15, the belief rules is obtained as follow:

$$\frac{SN \equiv \text{HloTS} \sim (N_s, N_h, (PID_{sh}^{new}, N_h, C_s)), SN \equiv \#(N_s, N_h)}{SN \equiv \text{HloTS} \equiv (N_s, N_h, (PID_{sh}^{new}, N_h, C_s))}$$

Because SN believes that HloTS once said $(N_s, N_h, (PID_{sh}^{new}, N_h, C_s))$ and SN believes that N_s, N_h are fresh, the SN believes that HloTS believes $(N_s, N_h, (PID_{sh}^{new}, N_h, C_s))$

$$\frac{SN \equiv \text{HloTS} \equiv (N_s, N_h, (PID_{sh}^{new}, N_h, C_s))}{SN \equiv \text{HloTS} \equiv (PID_{sh}^{new}, N_h, C_s)} \quad (\text{Goal 1})$$

Because SN believes that HloTS believes $(N_s, N_h, (PID_{sh}^{new}, N_h, C_s))$, SN believes that HloTS believes $(PID_{sh}^{new}, N_h, C_s)$

Based on formal analysis using the BAN logic and refers to **goals 1 to 4**, that our scheme achieves secure mutual authentication between Sensor Node (SN), Current Cluster Head (CCH), Home IoT server (HloTS). Therefore, all parties recognize the other party's identity by possessing the shared key K_{ch} , R_s and checking freshness based on N_s, N_h, N_c .

- a. *Execute*(π^{sn}, π^{hiots}): The equation denotes that the adversary can intercept all communication in the public channels between SN and HloTS . The model is called eavesdropping attack.
- b. *Send*(π^{sn}, m): Where the adversary has capabilities of sending a message to a participant, e.g., π^{sn} , and the adversary can both receive and reply. This query is called active attack
- c. *CorruptSensor*(π^{sn}): The adversary captures the sensor, and can extract the credential stored from the sensor's memory called stolen or lost device/smart card attack.
- d. *Test*(π^{sn}, π^{hiots}): The semantic security is determined by establishing the session key SK between SN π^{sn} and HloTS π^{hiots} by following the indistinguishability of ROR model [30]. The adversary first tosses an unbiased coin c and then results in an outcome of toss. If $c = 1$ denotes the new share key is fresh, hence, the adversary does not reveal (π^{sn}, π^{hiots}) , the session key SK . Otherwise, If the new share key is not fresh, π^{sn}, π^{hiots} returns a null and denotes the outcome of a random key.

5) Semantic Security of Session Key

In ROR model, the adversary must have the ability to distinguish both actual and random session key. The adversary is repeated for running *Test*() queries π^{sn} or π^{hiots} and stores the testing result in a bit c . If $c = c'$ denotes

that the adversary is a winner. Where c' represents the bit randomly guessed by the adversary. The ability of adversary to break semantic security from the Authentication Key Agreement protocol P in t specific time is defined $Adv_{P,A}^{AKE}(t) = |2 \cdot \Pr[SUCCESS] - 1|$, where $SUCCESS$ represents an event that adversary A wins the game.

6) Random Oracle

In our ROR model, the collision $h(\cdot)$ and secure $PUF(\cdot)$ can be accessed by the adversary and each participant.

7) Security Proof

The definition of secure PUF and Collision resistant-one-way-hash function is shown, and will be used to prove our semantic security scheme as follows.

Definition 1 (collision-resistant one-way hash function):

Formally, the definition of collision resistant-one-way hash function, $h: \{0,1\}^* \rightarrow \{0,1\}^n$ denotes the mathematical model of hash function output, where arbitrary length input of bit into hash function yields a fixed-length output's bit. The definition of adversary advantage to find the collision in time t is denoted by $Adv_A^{Hash}(t)$, where $Adv_A^{Hash}(t) = \Pr[(x_1, x_2) \in \mathcal{R}_A: x_1 \neq x_2, h(x_1) = h(x_2)]$, $\Pr(X)$ represents a probabilistic of X randomly; x_1, x_2 are strings randomly selected by A. The maximum execution time t of adversary (ϕ, t) success for attacking collision hash $h(\cdot)$ is denoted by $Adv_A^{Hash}(t) \leq \phi$.

Definition 2 (PUF function is secure)

The Secure PUF can be achieved, e.g., PUF_1 produces output responses of $R_1, R_2 \in \{0,1\}^k$ with at least d_1 variation for two input challenges of $C_1, C_2 \in \{0,1\}^k$, and if an input challenge C_1 produces distinct output responses of $R_1, R_2 \in \{0,1\}^k$ with at least d_2 variation for any two different PUFs (PUF_1, PUF_2). Therefore, $\Pr[HD(PUF_1(C_1), PUF_1(C_2)) > d_1] = 1 - \varepsilon$, $\Pr[HD(PUF_1(C_1), PUF_2(C_1)) > d_2] = 1 - \varepsilon$. ε is a negligible small value, the adversary selects the challenges randomly denoted by C_1, C_2 , HD is Hamming Distance and d_1, d_2 are the PUF's error tolerance thresholds.

By relying on the aforementioned **Definition 1** and **Definition 2** and acknowledging Zipf's law [31]. Theorem 1 results in a semantic security of the proposed protocol as follows.

Theorem 1: Let the adversary run an attack in the proposed protocol P at the polynomial-time under the ROR model. The user-chosen passwords based on Zipf's law [31], l_1, l_2 are the bits in secret R_s , ID_s is a secret user identity. The estimation of Adversary advantage breaks the semantic security of the protocol and reveals new share key between SN and HIoT as follows.

$$Adv_{P,A}^{AKE}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_p^2}{|PUF|} + 2 \max\{C' \cdot q_s^{s'}, \frac{q_s}{2^{l_1}}, \frac{q_s}{2^{l_2}}\}$$

Where q_h, q_p, q_s are respectively numbers of hash query, PUF query, and Sends query. $|Hash|$ is the range space of $h(\cdot)$, $|PUF|$ is range space of $PUF(\cdot)$, and C' and s' are Zipf's parameters [31].

Proof: in this article, we adopt similar proofs presented by [32], [33], and [34]. G_j denotes five sequence games, where $j \in [0,4]$. The Adversary A successes the guess bit c in game

G_j is represented by $SUCCESS$. The detail of game as follows.

Game G_0 : The game is considered an actual attack on protocol P by Adversary A under the ROR model. The beginning of game G_0 as follows:

$$Adv_{P,A}^{AKE}(t) = |2 \cdot \Pr[SUCCESS_0] - 1| \quad (1)$$

Game G_1 : Game 1 is an eavesdropping attack, Adversary A activates $Execute(\pi^{sn}, \pi^{hiots})$ hence A can intercept all transmitted messages, such as $M_1: \{PID_{sh}, N_s, ID_h, V_1\}$, $M_2: \{ID_{ch}, N_c^*, V_2, M_1\}$, $M_3: \{PID'_{sh}, N_h^*, C_s, V_3, V_4\}$, and $M_4: \{PID'_{sh}, N_h^*, C_s, V_4\}$. After that adversary A executes the Test to verify whether or not the result is the actual secret response or random number. In our protocol response generated from challenge where, $R_s = PUF(C_s)$. Only a legitimate sensor node can compute R_s . Therefore, the probability of Adversary A to win in G_1 by eavesdropping attack is not increased. Consequently, the results are as follows.

$$\Pr[SUCCESS_1] = \Pr[SUCCESS_0] \quad (2)$$

Game G_2 : game 2 simulates the Send q_h and Hash $|Hash|$ queries by modeling an active attack where Adversary A attempts to defraud the legitimate participants to accept the messages are modified by adversary A. Because all transmitted messages of $M_{A1}, M_{A2}, M_{A3}, M_{A4}$ are constructed using responses and no collision occurs when adversary A activates Send query q_h by helping $h(\cdot)$ query (See Definition 1). Based on the birthday paradox, the result is as follows:

$$|\Pr[SUCCESS_2] - \Pr[SUCCESS_1]| \leq \frac{q_h^2}{2|Hash|} \quad (3)$$

Game G_3 : This game has a similar argument with G_2 but the difference between G_3 and G_2 is that G_3 simulates the Send and PUF queries. Based on the secure PUF in Definition 2, the relationship is as follows.

$$|\Pr[SUCCESS_3] - \Pr[SUCCESS_2]| \leq \frac{q_p^2}{2|PUF|} \quad (4)$$

Game G_4 : in this final game, the adversary activates Corrupt Sensor, where adversary A can extract PID_{sh}, PID_{syn} , from the sensor. However, the adversary cannot obtain identity and response. The probability of guessing the response R_s of l_1 bits, and identity ID_s of l_2 bits are $\frac{1}{2^{l_1}}$ and $\frac{1}{2^{l_2}}$, respectively [31]. In addition, the adversary can guess the password based on Zipf's law [31]. If only guess the password, the adversary has an advantage of > 0.5 when $q_s = 10^7$ or 10^8 [31]. Therefore, if the attacker guess the password based on the user's identity, the adversary has an advantage of > 0.5 when $q_s \leq 10^6$ [31]. In actual conditions, the system does not allow many to try the incorrect passwords. Therefore, the game G_3 and G_4 have to indicate nothingness of the guessing attack. Thus, the result is as follows:

$$|\Pr[SUCCESS_4] - \Pr[SUCCESS_3]| \leq \max\{C' \cdot q_s^{s'}, \frac{q_s}{2^{l_1}}, \frac{q_s}{2^{l_2}}\} \quad (5)$$

In the final session, after activating the Test query, adversary A must guess bit c' to win game G_4 . Therefore, the result is as follows

$$\Pr[SUCCESS_4] = \frac{1}{2} \quad (6)$$

Based on equation (1), (2), and (6), we have

$$\frac{1}{2} Adv_{P,A}^{AKE}(t) = \left| \Pr[SUCCESS_0] - \frac{1}{2} \right|$$

$$= \left| \Pr[SUCCESS_1] - \frac{1}{2} \right|$$

$$= |\Pr[SUCCESS_1] - \Pr[SUCCESS_4]| \quad (7)$$

We get the following result by applying the triangle inequality and using equation (3), (4), and (5).

$$\begin{aligned} & |\Pr[SUCCESS_1] - \Pr[SUCCESS_4]| \\ & \leq |\Pr[SUCCESS_1] - \Pr[SUCCESS_3]| \\ & \quad + |\Pr[SUCCESS_3] - \Pr[SUCCESS_4]| \\ & \leq |\Pr[SUCCESS_1] - \Pr[SUCCESS_2]| \\ & \quad + |\Pr[SUCCESS_2] - \Pr[SUCCESS_3]| \\ & \quad + |\Pr[SUCCESS_3] - \Pr[SUCCESS_4]| \\ & \leq \frac{q_h^2}{|Hash|} + \frac{q_p^2}{|PUF|} \\ & \quad + 2 \max\{C' \cdot q_s', \frac{q_s}{2^{l_1}}, \frac{q_s}{2^{l_2}}\} \end{aligned} \quad (8)$$

Finally, we get the necessary result by solving equation (7) and (8):

$$Adv_{P,A}^{KE}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_p^2}{|PUF|} + 2 \max\{C' \cdot q_s', \frac{q_s}{2^{l_1}}, \frac{q_s}{2^{l_2}}\}$$

VII. FORMAL ANALYSIS USING SCYTHY TOOL.

This article also uses the Scyther tool as a formal analysis for validating the proposed protocol. Scyther tool is developed based on Python programming to verify the protocol security [35]. This tool also follows Delov-Yao (DY) adversary model

[29]. There are two steps for evaluating the protocol using this tool. Step 1, the protocol modeling is based on the Security Description Language (SPDL), and then Step 2 runs the tool to show the protocol security claims.

Figure 5 is a verification result from Scyther tool; it denotes that Scyther tool cannot find the attack. Hence, it can be said that our protocol withstands from various attacks based on the Scyther tool claim. Due to the limited size, this article does not show our protocol's programming model.

VIII. CONCLUSION

This article proposes a new protocol by preserving the untraceable and unclonable sensor movement using stable-PUF to improve the security features and resolve the distributed IoT environment problems. Based on the informal analysis, our proposed scheme has fulfilled the security features, such as Mutual Authentication, Untraceability, Anonymity, and protection against impersonation attacks, as well as protected from the cloning attacks (SF1-SF5). In addition, the formal analysis using BAN Logic ensures our scheme achieves the secure mutual authentication. The result of ROR model and Scyther tool show that our proposed scheme withstands from various kinds of attacks as well as proves and strengthens our informal analysis. On the other hand, based on the computational complexity comparison, our protocol obtains a lower computational cost than the schemes proposed by [15] and [19]. Therefore, our scheme is more suitable to be applied in the distributed IoT environment.

ACKNOWLEDGMENT

The author would like to thank the editors and all anonymous referees for their valuable inputs and suggestions.

REFERENCES

- [1] IBM, "IBM builds a smarter planet." [Online]. Available: <https://www.ibm.com/smarterplanet/us/en/>.
- [2] G. Montenegro, N. Kushalnagar, H. J. and C. D., "Transmission of IPv6 Packets over IEEE 802.15.4 Networks Status," *RFC4944*, pp. 1–30, 2007.
- [3] D. Guinard, M. Fischer, and V. Trifa, "Sharing Using Social Networks in a Composable Web of Things," *2010 8th IEEE Int. Conf. Pervasive Comput. Commun. Work. (PERCOM Work.)*, pp. 702–707, 2010.
- [4] Libelium, "Interfacing the Sensor Networks With the Web 2.0." [Online]. Available: <https://www.libelium.com/>.
- [5] D. Mandl *et al.*, "Sensor Web 2.0 : Connecting Earth's Sensors via the Internet," no. January, 2008.
- [6] C. P. Mayer, "Security and Privacy Challenges in the Internet of Things," *Electron. Commun. EASST Work. der Wissenschaftlichen Konf. Kommun. Verteilten Syst. 2009 (WowKiVS 2009)*, no. January 2009, 2013.
- [7] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.
- [8] F. Zhu, M. W. Mutka, and L. M. Ni, "Private Entity Authentication for Pervasive Computing Environments," *Int. J. Netw. Secur.*, vol. 14, no. 2, pp. 86–100, 2012.
- [9] S. Shin, T. Shon, H. Yeh, and K. Kim, "An effective authentication mechanism for ubiquitous collaboration in heterogeneous computing environment," *Peer-to-Peer Netw. Appl.*, vol. 7, pp. 612–619, 2014.
- [10] P. Gope and T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," *IEEE Sens. J.*, vol. 15, no. 9, pp. 5340–5348, 2015.

Scyther results : verify					
Claim			Status	Comments	
ideal_PUF_Unclonable	SN	ideal_PUF_Unclonable,SN1	Secret IDs	Ok	No attacks within bound
		ideal_PUF_Unclonable,SN2	Secret PUF(Cs)	Ok	No attacks within bound
		ideal_PUF_Unclonable,SN3	Niagree	Ok	No attacks within bound
		ideal_PUF_Unclonable,SN4	Nisynch	Ok	No attacks within bound
		ideal_PUF_Unclonable,SN5	Alive	Ok	No attacks within bound
		ideal_PUF_Unclonable,SN6	Weakagree	Ok	No attacks within bound
CCH		ideal_PUF_Unclonable,CCH1	Secret Kch	Ok	No attacks within bound
		ideal_PUF_Unclonable,CCH2	Niagree	Ok	No attacks within bound
		ideal_PUF_Unclonable,CCH3	Nisynch	Ok	No attacks within bound
		ideal_PUF_Unclonable,CCH4	Alive	Ok	No attacks within bound
		ideal_PUF_Unclonable,CCH5	Weakagree	Ok	No attacks within bound
		ideal_PUF_Unclonable,CCH6	Weakagree	Ok	No attacks within bound
HioTs		ideal_PUF_Unclonable,HioTs1	Secret IDs	Ok	No attacks within bound
		ideal_PUF_Unclonable,HioTs2	Secret PUF(Cs)	Ok	No attacks within bound
		ideal_PUF_Unclonable,HioTs3	Niagree	Ok	No attacks within bound
		ideal_PUF_Unclonable,HioTs4	Nisynch	Ok	No attacks within bound
		ideal_PUF_Unclonable,HioTs5	Alive	Ok	No attacks within bound
		ideal_PUF_Unclonable,HioTs6	Weakagree	Ok	No attacks within bound

Fig. 5. Results of verification to the proposed protocol using Scyther Tool

- [11] Y. Liu, S. Member, J. Li, and S. Member, "PKC Based Broadcast Authentication using Signature Amortization for WSNs," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 6, pp. 2106–2115, 2012.
- [12] T. Kwon and J. Hong, "Secure and Efficient Broadcast Authentication in Wireless Sensor Networks," *IEEE Trans. Comput.*, vol. 59, no. 8, pp. 1120–1133, 2010.
- [13] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security," *Internet Engineering Task Force (IETF)*, 2006. [Online]. Available: <https://tools.ietf.org/html/rfc4347>. [Accessed: 17-Dec-2020].
- [14] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," *Internet Engineering Task Force (IETF)*, 2014. [Online]. Available: <https://tools.ietf.org/html/rfc7252>. [Accessed: 17-Dec-2020].
- [15] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things q," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.
- [16] X. H. Le *et al.*, "An Energy-Efficient Access Control Scheme for Wireless Sensor Networks based on Elliptic Curve Cryptography," *J. Commun. networks*, vol. 11, no. 6, pp. 599–606, 2009.
- [17] M. Hwang, Y. Chu, I. Engineering, and T. H. Road, "AN EFFICIENT SENSOR-TO-SENSOR AUTHENTICATED PATH-KEY ESTABLISHMENT SCHEME FOR SECURE COMMUNICATIONS IN WIRELESS SENSOR NETWORKS," *Int. J. Innov. Comput. Inf. Control*, vol. x, no. 0, pp. 1–16, 2009.
- [18] P. Kotzanikolaou and C. Douligeris, "Hybrid Key Establishment for Multiphase Self-Organized Sensor Networks A Hybrid Key Establishment Protocol for," *Sixth IEEE Int. Symp. a World Wirel. Mob. Multimed. Networks*, 2005.
- [19] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey : A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications," *Int. J. Distrib. Sens. Networks*, vol. 2014, 2014.
- [20] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," *2007 44th ACM/IEEE Des. Autom. Conf. San Diego*, pp. 9–14, 2007.
- [21] C. Bohm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. New York: NY, USA: Springer, 2012.
- [22] P. Tuyls and L. Batina, "RFID-Tags for Anti-counterfeiting," *Top. Cryptol. CT-RSA (LNCS 3860)*, Heidelberg, Ger. Springer, pp. 115–131, 2006.
- [23] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors : How to Generate Strong Keys from Biometrics and Other Noisy Data," *Adv. Cryptology—EUROCRYPT2004 (Lecture Notes Comput. Sci. Heidelberg, Ger. Springer*, pp. 523–540, 2004.
- [24] D. Jeon, J. H. Baek, D. K. Kim, and B. Choi, "Toward Zero Bit-Error-Rate Physical Unclonable Function : Mismatch-Based vs . Physical-Based Approaches in Standard CMOS Technology," *2015 Euromicro Conf. Digit. Syst. Des.*, pp. 407–414, 2015.
- [25] K. Chuang *et al.*, "A Physically Unclonable Function Using Soft Oxide Breakdown Featuring 0 % Native," *IEEE J. Solid-State Circuits*, vol. 54, no. 10, pp. 2765–2776, 2019.
- [26] P. P. Crystals, X. Lu, S. Member, L. Hong, and S. Member, "CMOS Optical PUFs Using Noise-Immune Incorporating Passive Variations," *IEEE J. Solid-State Circuits*, vol. 53, no. 9, pp. 2709–2721, 2018.
- [27] W. Wang, Y. Yona, S. N. Diggavi, and P. Gupta, "Design and Analysis of Stability-Guaranteed PUFs," *IEEE Trans. Inf. FORENSICS Secur.*, vol. 13, no. 4, pp. 978–992, 2018.
- [28] M. Burrows and R. Needham, "A Logic of Authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, 1989.
- [29] D. Dolev, "On the Security of Public Key Protocols," *IEEE Trans. Inf. THEORY*, no. M, pp. 198–208, 1983.
- [30] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-Based Authenticated Key Exchange in the Three-Party Setting," *IACR Int. Conf. Public-Key Cryptogr.*, vol. 3386, pp. 65–84, 2005.
- [31] D. Wang, S. Member, H. Cheng, P. Wang, and S. Member, "Zipf's Law in Passwords," *IEEE Trans. Inf. FORENSICS Secur.*, vol. 12, no. 11, pp. 2776–2791, 2017.
- [32] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless," *IEEE Trans. Ind. INFORMATICS*, vol. 15, no. 9, pp. 4957–4968, 2019.
- [33] S. Roy *et al.*, "Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications," *IEEE Trans. Ind. INFORMATICS*, vol. 15, no. 1, pp. 457–468, 2020.
- [34] S. Roy, S. Chatterjee, A. K. Das, and S. Chattopadhyay, "On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services," *IEEE Access*, no. October, 2017.
- [35] C. Cremers, "The Scyther Tool : Verification , Falsification , and Analysis of Security Protocols," *Proc. Int. Conf. Comput. Aided VeriFcation*, pp. 1–4.

E Haodudin Nurkifli received the bachelor degree of Engineering (S.T.) from The Faculty of Engineering, Universitas Ahmad Dahlan (UAD), Indonesia, in 2008, and Master degree (M.Cs.) in Computer Science from Universitas Gadjah Mada (UGM), Indonesia, in 2012. He is currently pursuing a doctoral degree (Ph.D.) in computer science and information engineering from the National Cheng Kung University (NCKU), Tainan, Taiwan. He is also working as a research assistant at NCKU and a lecturer at Universitas Singaperbangsa Karawang, Indonesia. His research primarily focuses on cryptography, authentication, and security in IoT, IoV, Smart Grid, WSN environment, and PUF-based hardware security.