Untraceable Sensor Movement in Distributed IoT Infrastructure

Prosanta Gope and Tzonelih Hwang

***Abstract*— Recent advances in information and communication technologies and embedded systems have given rise to a new disruptive technology, the Internet of Things (IoTs). IoT allows people and objects in the physical world as well as data and virtual environments to interact with each other so as to create smart environments, such as smart transport systems, smart cities, smart health, and so on. However, IoT raises some important questions and also introduces new challenges for the security of systems and processes and the privacy of individuals, such as their location and movements and so on. In this paper, at first, we propose a distributed IoT system architecture. Subsequently, we propose an anonymous authentication scheme, which can ensure some of the notable properties, such as sensor anonymity, sensor untraceability, resistance to replay attacks, cloning attacks, and so on. It is argued that the proposed authentication scheme will be useful in many distributed IoT applications (such as radio-frequency identification-based IoT system, Biosensor-based IoT healthcare system, and so on), where the privacy of the sensor movement is greatly desirable.**

***Index Terms*— Internet of Things, privacy, anonymity, untraceability, wireless sensor network.**

I. Introduction

WIRELESS sensor network (WSN) is one of the indispensable elements in the IoT paradigm. The benefits of connecting both WSN and other IoT elements go beyond remote access, as heterogeneous information systems can be able to collaborate and provide common services. This integration is not mere speculation, but a fact supported by several international companies. Noteworthy examples are 'A Smarter Planet' [1], a strategy developed by IBM which considers sensors as fundamental pillars in intelligent water management systems and intelligent cities; and the CeNSE project by HP Labs, focused on the deployment of a worldwide sensor network in order to create a "central nervous system for the Earth". At the same time, the technologies that will enable the integration are being developed and tested. For example, the 6LowPAN standard, defined by IETF [2], allows the transmission of IPv6 packets through computationally restricted networks. Moreover, it is actually possible to link the data produced by the elements of a WSN (sensor nodes) with web services based on SOAP and REST [3], messaging mechanisms (such as emails and SMS) or social networks (e.g. Twitter) and blogs (e.g. WordPress) [4]. However, having IP connectivity does not mean that every sensor node should be directly connected to the Internet. There are many challenges that must be carefully considered, and one of those challenges is security and privacy of the sensor node in IoT infrastructure. Precisely, there are some IoT based applications like healthcare system, where movement or status of a patient can be identified by the sensors. In some cases, it is highly desirable to maintain privacy of the patient's movement. For example, considering that a high profile patient (possibly a politician) has been admitted to a hospital and the patient may have to move several rooms and even several buildings of the hospital for pathological tests or treatment with a bio-sensor or a Radio-frequency identification (RFID) based tag sensor, assigned by the hospital authority, where the sensor will help the patients to prove his/her legitimacy. That is, whether the patient can enter into a particular area or not. In that case, because of the security reason movement of patients should be kept secret.

Now, in order to allow WSN to become an intrinsic part of the IoT in a secure way, several security challenges [5], [6] are required to be considered. However, in this paper we focus on the privacy of the sensor movement in a distributed IoT infrastructure. In this regard, at first we propose a distributed IoT system architecture. Then, we design a lightweight anonymous authentication scheme, which can guarantee various security issues related to privacy of the sensor node like anonymity, untraceability, replay attacks, DoS attacks, etc. In order to design the lightweight authentication framework for IoT, we will use the lightweight cryptographic primitives like the hash function and bitwise exclusive-OR, where these cryptographic primitives cause less computational overhead and reasonably much less execution time as compared to other cryptographic primitives like asymmetric encryption/decryption, modulo operation etc., which is highly adequate for the tiny-powered sensor node (shown in Section VI).

Paper Organization: The rest of the paper is organized as follows. Section II provides a brief overview about the related work. In Section III, we comprehensively describe our proposed distributed IoT system architecture. In Section IV, we provide our anonymous authentication scheme, which can guarantee privacy of a sensor movement. Security analysis of the proposed scheme is given in Section V. A relevant

Manuscript received March 2, 2015; revised June 1, 2015; accepted June 2, 2015. Date of publication June 9, 2015; date of current version July 24, 2015. This work was supported by the National Science Council of Taiwan under Contract MOST 103-2221-E-006-177. The associate editor coordinating the review of this paper and approving it for publication was Prof. Subhas C. Mukhopadhyay. *(Corresponding author: Tzonelih Hwang.)*

The authors are with the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan 701, Taiwan (e-mail: prosanta.nitdgp@gmail.com; hwangtl@ismail.csie.ncku.edu.tw).

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

Digital Object Identifier 10.1109/JSEN.2015.2441113

TABLE I
NOTATIONS AND CRYPTOGRAPHIC FUNCTIONS

Symbol	Definition
Sn	Sensor Node
CH	Cluster Head
HIoTS	Home IoT Server
ID_{Sn}	Identity of the Sensor
AID_{Sn}	One-time-alias Identity of the Sensor
SID	Shadow Identity of Sensor
H_{id}	Identity of the HIoTS
N_s	Random number generated by the Sensor Node
K_{sh}	Shared key between Sn and HIoTS
K_{ch}	Secret Key Shared between the CH and HIoTS
Tr_{seq}	Track sequence number (maintain both Sn and HIoTS)
$h(.)$	One-way hash function
$\oplus$	Exclusive-OR operation
$\|$	Concatenation operation

discussion based on the performance of the proposed scheme is given in Section VI. The formal analysis of the proposed scheme is presented in Section VII. Finally, concluding remark is given in Section VIII. The abbreviations and cryptographic functions used in this article are defined in the Table 1.

II. RELATED WORK

Distributed architecture supports the IoT network application by providing services at local level and collaborating with all the network devices and users to achieve common goals. Because of the network heterogeneity and device mobility, there can be many security threat and issues encountered with the distributed IoT. In [7] Roman et al. identified security challenges in distributed IoT. Based on their study, identity of the network entity, authentication, untraceability, and access control are the major security concerns in distributed IoT. The proposed mechanism should be robust to node mobility and network scalability due to the dynamic behavior of the nodes. Precisely, a sensor node can travel one cluster to another cluster and even can travel one network to another. Therefore, the proposed scheme should be robust to sensor node mobility.

Exploitation of a master key for entity authentication for pervasive computing environments would be a feasible approach to IoT enabled WSNs [8]. According to [9], the authentication mechanism for WSN applications can be summarized as password based remote authentication using ticket. However, most of the work has sole purpose of enabling end-user authentication in generic WSN architecture and it does not provide the extensibility for the key establishment which is greatly important for secure communication. In [10] and [11], the authors proposed broadcast authentication protocol for WSN. Another ticket based authentication mechanism was proposed in [9], for ubiquitous collaboration in heterogeneous computing environment, which is not applicable to the high resource constrained device due to the large memory consumption. Datagram Transport Layer Security (DTLS) is an adaptation of TLS protocol and it provides an equal communication security TLS diagram protocols [12]. According to [13], the secured version of CoAP (Constrained Application Protocol) is defined with DTLS due to the unreliable communication like in CoAP based IoT networks. In [14], the authors have introduced the first fully implemented two way authentication scheme for IoT. However, due to the eight message transfers to complete DTLS handshake, it includes a significant overhead to the network traffic. The main drawback is the utilization of X.509 certificates and RSA public key with DTLS handshake which are too heavy for low performing and high resources restricted sensor nodes. Apart from these protocols, some other authentication protocols [15]–[18] have also been proposed where most of them are based on either elliptic curve digital signature algorithm (ECDSA) or elliptic curve Diffie-Hellman (ECDH). However, these are the protocols cause higher computational overhead which is not adequate for a tiny-powered sensor nodes. Nevertheless, none of the aforesaid authentication protocol supports the properties such as anonymity, and untraceability of the sensor nodes, which are greatly imperative, especially in the sense of their location privacy and movement.

III. PROPOSED DISTRIBUTED IOT SYSTEM ARCHITECTURE

In this section, we provide details about the proposed distributed IoT system architecture, where our anonymous authentication scheme is modeled. Fig 1, illustrates the proposed network architecture for the proposed lightweight anonymous authentication scheme. There are four indispensable components in our distributed IoT system architecture: an authenticated cloud server (ACS), two types of network entities such as cluster head (CH) and home IoT server (HIoTS), and edge devices (sensor nodes). All the edge devices and the cluster heads need to register into a particular HIoTS. In that case, the edge devices and cluster heads will get security credentials from the HIoTS. On the other hand, every end user and HIoTS needs to register into ACS. When two HIoTS need to interact with each other, then ACS will help them for authenticating each other and to establish the shared security credentials or establishing a secure communication link between them. Besides, when an end user needs to access some real-time data from a sensor node, which is available at a HIoTS, then the HIoTS server needs to authenticate the end user with the help of ACS. Note that, even though there are several issues those are required to be considered in our proposed distributed IoT model. However, because of the space limitation, in this article we will be emphasizing on the issue of secure sensor movement in the proposed distributed IoT infrastructure, which is an important issue for various distributed IoT applications. In this context, every HIoTS, which is basically a gateway, is responsible to authenticate the sensor node, especially when the sensor node moves

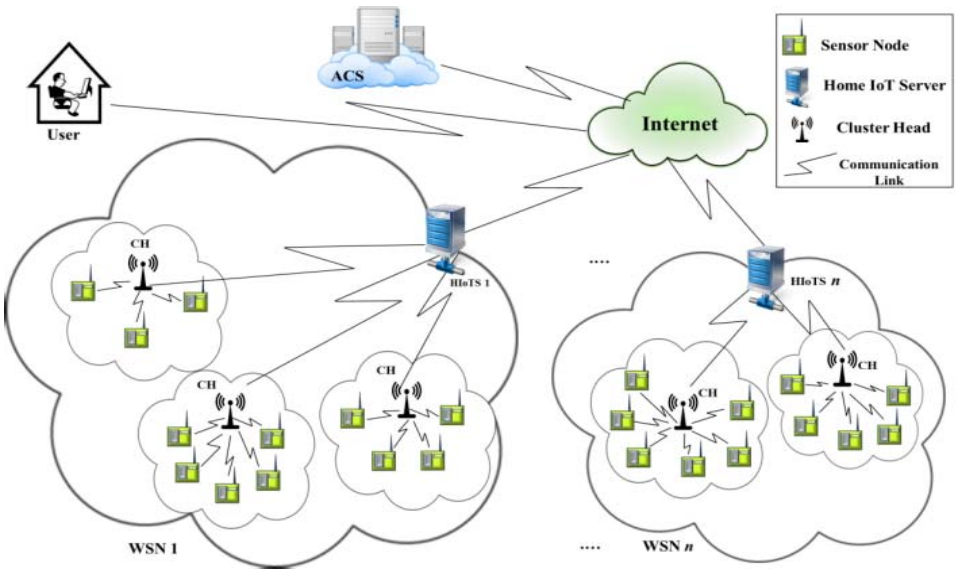


Fig. 1. Proposed distributed IoT system architecture.

from one cluster to another or moves from one network to another network. Only the particular HIoTS where the sensor node has been registered can know the sensor's original identity and movement. On the other hand, in our proposed system architecture each cluster head works like a relay. In that case, their task is to convey the sensor encoded information to the HIoTS that they (cluster heads) belong to. Now, when a sensor node moves from one cluster to another then the cluster head verifies the sensor node with the help of the HIoTS and then decides whether the sensor node can enter or join into the cluster or not. On the other hand, when the sensor node moves from one WSN to another then, the current HIoTS needs to asks the original HIoTS of the sensor node, where the sensor node is registered, for the legitimacy of the sensor node and based on its (sensor node) HIoTS response only the current HIoTS can decide that whether the sensor node can enter to its region or not.

Our proposed system architecture can be useful in several distributed IoT applications such as RFID based distributed IoT applications, where a person having RFID tag sensor can move between several building blocks. In that case, our cluster head will be treated as a TAG reader and HIoTS will be considered as a backend database server. Besides, our proposed system model can also support the healthcare based distributed IoT applications, where a patient having bio-sensor may have to travel several areas and the sensor needs to periodically send the status of the patient to the HIoTS that it belongs to. In that case, the current cluster head and current HIoTS needs to help the bio-sensor to send its private information. However, for maintaining the security of the entire system, it's the responsibility of the cluster head and the HIoTS servers to authenticate the bio-sensor. Nevertheless, our proposed distributed IoT system architecture also supports the mobile-IoT applications, where the cluster head will be considered as foreign agent and the HIoTS, sensor will be considered as home agent and the mobile sensor, respectively. In that case, any foreign agent that the mobile user visits, needs to authenticate the mobile user by using the support of his/her home agent.

IV. Proposed Anonymous Authentication Scheme

In this section, we will describe our proposed anonymous authentication scheme in detail. Our proposed scheme consists of three phases. In Phase I, a home IoT server (HIoTS) issues security credentials to a sensor node through secure channel, this phase is called registration phase. In the next phase of our proposed scheme (Phase II), we design an anonymous authentication protocol for inter cluster movement of the sensor node, where a sensor node (ID_{Sn_i}) remain in the same WSN that it belongs to, but it may move from one cluster to another. So, this phase can be represented as inter-cluster movement phase. In the Phase III of our proposed scheme, we present the anonymous authentication environment for inter-network movement of the sensor node. Therefore, this phase is denoted as the inter-network movement phase. So, the design objectives of our proposed scheme are as follows:

- To achieve mutual authentication by preserving the feature of anonymity of the sensor node;
- To achieve untracebilty;
- To defeat forgery attack, and cloning attack.
- To reduce computation and communication cost;

A. Phase I: Registration Phase

A sensor node sends its identity ID_{Sn_i} to a home IoT server (HIoTS) in a secure manner. After receiving the request from sensor node, the HIoTS generates a random number n_h and then computes $K_{sh} = h(ID_{Sn_i} \| n_h) \oplus H_{id}$. Subsequently, HIoTS also generates a set of unlinkable shadow-IDs $SID = \{sid_1, sid_2, \ldots\}$, where for each $sid_j \in SID$, HIoTS computes $sid_j = h(ID_{Sn_i} \| r_j \| K_{sh})$. Here, the parameter r_j denotes the random numbers used for

deriving the shadow-ID sid_j. Hereafter, the HIoTS generates a track sequence number Tr_{seq}, which is basically a sequence number of 32-bit. This sequence number is randomly generated. Precisely, the system generates a random number m and then sets $Tr_{seq} = m$ and subsequently sends Tr_{seq} to the sensor node by keeping a copy in its database, in which HIoTS can see the most recent Tr_{seq} for each sensor node registered into the system. This sequence number is used to speed up the authentication process as well as to prevent any replay attempt from any adversary, where by seeing the Tr_{seq} and comparing it with the stored value of its database, the HIoTS can comprehend the sensor node and based on Tr_{seq}, the gateway HIoTS can even decide that whether the request is valid or not. Precisely, during the execution of the anonymous authentication in Phase II and Phase III, if the Tr_{seq} provided by the sensor node does not match with the stored value of the HIoTS's database. Then, the HIoTS will immediately terminate the connection. In that case, sensor node will be asked to use its one of the unused shadow identity $sid_j \in SID$. Once a shadow-ID sid_j is used up from the list of (SID), then the (sid_j) must be deleted from the list by both the sensor node and HIoTS. Now, the HIoTS securely sends $\{K_{sh}, (SID), Tr_{seq}h(.)\}$ to the sensor node through the secure channel; and then the HIoTS stores a copy of ID_{Sn_i}, K_{sh}, SID, and Tr_{seq} in its own database for further communication.

B. Phase II: Anonymous Authentication in Inter-Cluster Movement Phase

In this phase of the proposed scheme, we consider the sensor movements from one cluster to another. In that case, it is the responsibility of the visiting or current cluster head, to authenticate the sensor node with the help of the HIoTS. Therefore, this phase achieves goal of authentication among the sensor node, HIoTS, and the current cluster head (CH). This phase of the proposed scheme consists of the following steps:

Step 1 M_{A_1} $\{AID_{Sn},\ N_x,\ Tr_{seq}(if\ req.),\ H_{id},\ V_1\}$*:* The sensor node ID_{Sn_i} generates a random number N_s and derives $AID_{Sn} = h(ID_{Sn_i} \| K_{sh} \| N_s \| Tr_{seq})$, $N_x = K_{sh} \oplus N_s$, and $V_1 = h(AID_{Sn} \| K_{sh} \| N_x \| H_{id})$. Finally, the sensor node forms a request message M_{A_1} and then sends it to cluster head (CH). Here, Tr_{seq} denotes the most recent track sequence number received from the HIoTS (H_{id}). Note that, in case of loss of synchronization, the sensor node needs to choose one of the unused sid_j and subsequently, assigns the sid_j as AID_{Sn} i.e. $AID_{Sn} = sid_j$. In that case, the sensor node need not to send any track sequence number Tr_{seq} in M_{A_1}.

Step 2 M_{A_2} $\{N_y, ID_{ch_j}, V_2, M_{A_1}\}$*:* After receiving the request from the sensor node, the cluster head (CH) generates a random number N_c and computes $N_y = K_{ch} \oplus N_c$, $V_2 = h(\mathrm{M_{A_1}} \| N_c \| K_{ch})$. Finally, the cluster head forms a request message M_{A_2} and sends it to the HIoTS.

Step 3 M_{A_3} $\{Tr, V_3, V_4\}$*:* Upon receiving the request message from cluster head, the HIoTS at first checks whether the track sequence number Tr_{seq} is valid or not and simultaneously also computes and checks whether V_1 is equal to $h(AID_{Sn} \| K_{sh} \| N_x \| H_{id})$or not. If so, then the HIoTS at first derives $N_s = K_{sh} \oplus N_x$, and then verifies AID_{Sn}. Otherwise, the HIoTS terminates the connection of the protocol.

Now, if the verification of AID_{Sn} is successful, then the HIoTS generates a random number m and assigns $Tr_{seq_{new}} = m$. Subsequently, the HIoTS computes $Ts = h(K_{sh} \| ID_{Sn_i} \| N_s) \oplus Tr_{seq_{new}}$, $V_4 = h(Tr \| K_{sh} \| ID_{Sn_i})$, $V_3 = h(ID_{Ch_j} \| N_c \| K_{ch})$ and forms a response message M_{A_3} and sends it to the cluster head.

Step 4 M_{A_4} $\{Tr, V_3\}$*:* After receiving the response message M_{A_3}, the cluster head computes $h(ID_{Ch_j} \| N_c \| K_{ch})$ and checks whether it is equals to V_3 or not. If so, then cluster head forms a response message M_{A_4}, and sends it to the sensor node. Otherwise, the cluster head will terminates the connection. Upon receiving the response message M_{A_4}, the sensor node computes $h(Tr \| K_{sh} \| ID_{Sn_i})$ and verifies whether it is equals to V_4 or not. If so, then the sensor node derives $Tr_{seq_{new}} = h(K_{sh} \| ID_{Sn_i} \| N_s) \oplus Tr$ and stores $Tr_{seq} = Tr_{seq_{new}}$ for further communication. Otherwise, the sensor node needs to start with a new request with an unused shadow identity. Note that, in case if the gateway cannot find any Tr_{seq} in $\mathrm{M_{A_1}}$, then the system (HIoTS), will validate the AID_{Sn} first, where the system will try to recognize the sid_j in AID_{Sn}. If so, then only the system proceeds for any further computation. If the system cannot recognize the sid_j in AID_{Sn} then it terminates the connection and requests the sensor to try with a valid shadow identity sid_j.

Now, in our proposed scheme, both the shadow identity and one-time alias identity with transaction sequence number can resolve the issues like user anonymity and untraceability. However, since the usage of (shadow-ID) in every transaction may cause excessive storage cost in both the sensor node and HIoTS. Therefore, the concept of (shadow-ID) we only use for dealing with the DoS attack [19], [20], which may occur because of the loss of synchronization between sensor and gateway HIoTS. That can be comprehended if the response message $\mathrm{M_{A_4}}$ has been interrupted, so that the sensor node cannot receive the message within a specific time period. In that case, only a reasonable number of shadow-identities are required to be stored. Although the attackers can continuously interrupt the connections to destroy the unlinkability, it is the trade-off problem. The system can limit the failure for updating track sequence numbers. In case, when all the pairs have already been used up then the HIoTS will securely send a new set of *SID* to the sensor node. Now, if there is any check in the above steps is invalid this phase of the proposed scheme will be aborted. On the other hand, successful completion of this phase indicates that both the cluster head and sensor node proof their legitimacy to the gateway HIoTS. The details of the authentication procedures of this phase are also depicted in Fig. 2.

C. Phase III: Anonymous Authentication in Inter-Network Movement Phase

In this phase of the proposed scheme, we consider the sensor movements from one WSN to another. In that case, it is the responsibility of both the visiting or current cluster

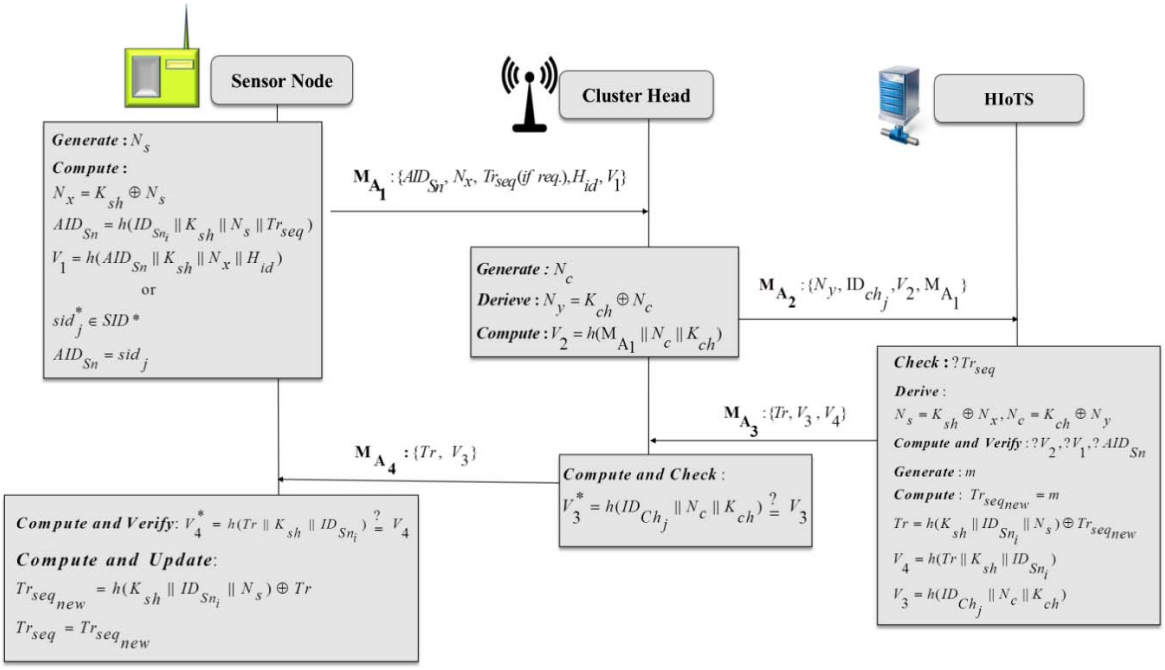


Fig. 2. Anonymous authentication for inter-cluster sensor movement.

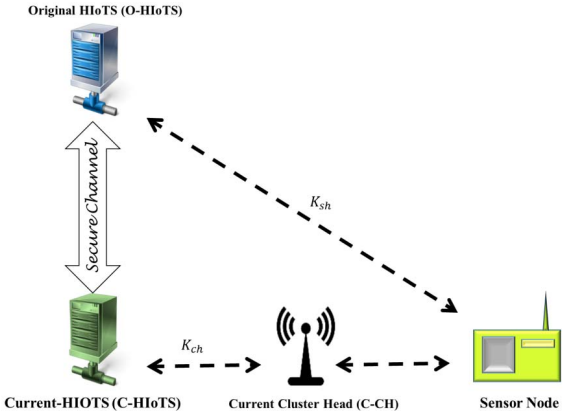


Fig. 3. Anonymous authentication environment for inter-network sensor movement.

head (C-CH) and the visiting or current HIoTS (C-HIoTS), to authenticate the sensor node with the help of the original HIoTS (O-HIoTS), where the sensor has been registered. Fig 3 illustrates the environment in details. Here, we assume that both the HIoTS servers maintain a secure channel for their interaction, which has been established with help of ACS. Now, in order to authenticate the sensor node, the similar protocol of Phase II can be used with the minor changes. In that case, when the C-HIoTS receives the message M_{A_2} then the system checks H_{id} with its own identity number. If the system founds that H_{id} does not match, then it forwards the M_{A_1} parts of the message M_{A_2} to the intended HIoTS (referred in H_{id}) through the secure channel. After receiving the M_{A_1}, the system (O-HIoTS) verifies the track sequence number Tr_{seq} is valid or not and simultaneously it also checks the parameters V_1, and AID_{Sn}. If the verification is successful, then the O-HIoTS generates and sends $\{Tr, V_3\}$ to the C-HIoTS for sensor node. Otherwise, it terminates the connection request. Upon receiving $\{Tr, V_3\}$, the C-HIoTS generates V_4 and sends it with $\{Tr, V_3\}$ to the cluster head (C-CH). The rest of the authentication procedures are similar as discussed in Phase II.

V. Security Analysis

In this section, we will demonstrate that our proposed scheme holds several imperative security properties, which are indeed essential for securing wireless sensor networks based IoT environment.

A. Accomplishment of the Mutual Authentication

Proof: In our *Anonymous Authentication* Phase II and Phase III of the proposed scheme, where the gateway HIoTS or O- HIoTS authenticates the sensor node $IDSn_i$ by verifying the one-time-alias $AIDSn$, and V_1 in the request message M_{A_2}. Whereas, the gateway authenticates the cluster head $IDCh_j$ using the value of the parameter V_2 in the request message M_{A_2}, which must be equal to $h(M_{A_1} \| N_c \| K_{ch})$. On the other hand, the sensor node authenticates the HIoTS by using the value V_4 in M_{A_4} and similarly the cluster head authenticates the HIoTS by verifying the hash value V_3 in M_{A_3}, which must be equal to $h(IDCh_j \| N_c \| K_{ch})$. In this way, all the participants of the proposed scheme mutually authenticate each other's.

B. Accomplishment of the Sensor Anonymity and Untraceability

Proof: As we mentioned before that both the shadow identity and one-time-alias identity with transaction sequence number can resolve the issues like user anonymity and untraceability. There is not direct relationship between the

aliases. Besides, it can also be noticed that during the execution of our anonymous authentication protocols in Phase II, and Phase III none of the parameter in the request message M_{A_1} is allowed to be sent twice. This approach of the proposed scheme is quite effective for privacy against eavesdropper (PAE) [21] to achieve along with the features of sensor anonymity and untraceability, where only the concerned HIoTS, in which the sensor has been registered, can track the sensor movement.

C. Accomplishment of Scalability

Proof: It is essential that an authentication scheme should be scalable. To authenticate the sensor node, the gateway HIoTS or O-HIoTS has to find matching records from its database. If the computational workload of the searching algorithm increases significantly as the number of sensor nodes increases, the system will not scale. Now, in the existing anonymous authentication protocols for a distributed for IoT system such as RFID [22]–[26], where a database server need to perform any exhaustive search operation in order to figure out the identity of a RFID tag sensor, which is not relevant at all. In order to justify our point more clearly, here we consider an example, in case of the protocol like [25], where we can see that when a tag sensor requests with a random number r_T then the reader responses with $\{r_R, ID_R\}$, where r_R is the random number generated by the reader and ID_R denotes the identity of the reader. Then the tag sensor sends the request message $\{h(ID_R\|s)_m, h(ID_R\|s\|r_R\|r_T) \oplus ID_T$ to the reader, where ID_T denotes the identity of the tag sensor and s is the tag sensor secret shared between the reader's backend database server and the tag sensor (each tag has its own secret s), and the parameter m denotes the number of bits. Now, when the reader's backend database server receives the request message then the server needs to figure out the tag information. However, none of the parameter can help the database server to comprehend the tag information such as identity. In order to know the tag identity either the database server needs to perform an exhaustive search operation by targeting the relation $h(ID_R\|s\|r_R\|r_T) \oplus ID_T$ or both the database server and tag may require to manage a backend channel for that. Unfortunately, the similar problem can also be profound in other existing state of the art lightweight authentication protocols [22]–[24], [26]. In our proposed scheme the HIoTS server need not to perform any exhaustive search operation. Instead of that, by checking the most recent track sequence number Tr_{seq} or a valid shadow identity sid_j, the HIoTS can respond quickly to the request of the sensor node, which makes our proposed scheme more saleable.

D. Resistance to Impersonating Attacks

Proof: This is a kind of forgery problem that arises when an attacker impersonating a sensor node or HIoTS or a cluster head (CH) is verified as a legitimate object and exploits this by performing other attacks like replay attacks. Now, in our proposed scheme, only a legitimate sensor node ID_{Sn_i} can form an authentic request message M_{A_1} with the valid one-time-alias AID_{Sn}, Tr_{seq}, and V_1. In order to do that, the attacker needs to know secret key K_{sh}. Similarly, only the legitimate cluster head and HIoTS can form the valid message M_{A_2} and M_{A_3}, respectively. In order to do that, attacker needs to know the secret security credentials such as K_{ch} and K_{sh}. In this way, our proposed scheme can resist impersonating attacks.

E. Resistance to Replay Attacks

Proof: Having intercepted previous communication, the attacker can replay the same message of the receiver or the sender to pass the verification process of the system. In our proposed scheme, none of the parameter in the request message M_{A_1} is allowed to be sent twice. Hence, if the attacker tries to intercept and resend the same request message, then by using the most recent track sequence number or the valid shadow identity, it will be easily detected by the HIOTS. In similar way, if the attacker attempts to send the same response message M_{A_4}, then the tag can easily comprehend that, in that case the value of V_4 will not be equal to the $h(Tr\|K_{sh}\|ID_{Sn_i})$. In this way, our proposed scheme can resist any replay attacks.

F. Resistance to Cloning Attacks

Proof: If a group of sensor nodes share the same key and use it for authentication, then it is vulnerable to cloning attacks [27]. In our proposed scheme, each sensor node owns its unique secret credentials $\{K_{sh}, (SID), Tr_{seq}\}$. If one of the sensor nodes is captured, the attacker cannot use the know secrets to derive the secrets of some other sensor node. That is, the attacker cannot use the revealed secret to clone some other sensor nodes. In this way, our proposed scheme can resist the cloning attack.

VI. Performance Analysis and Comparisons

The purpose of the proposed scheme is to resolve various security issues related to privacy of the sensor node especially in WSN based distributed IoT applications. In this section, we compare our proposed scheme with two recently proposed authentication mechanism for WSNs in distributed IoT infrastructure [14], [18] to manifest the advantages of our proposed scheme. We also demonstrate that our proposed scheme is well suitable for tiny-powered sensor devices. Now, in order to analyze the performance of our proposed scheme especially on the security front, our proposed scheme has been compared with two state of the art protocols [14], [18] (shown in Table II). From TABLE II, it is clear that the proposed scheme can satisfy all the properties. In contrast, the protocols presented in [14] and [18] cannot ensure the security properties such as anonymity, untraceability [28], etc. which are greatly imperative for keeping privacy of the sensor movement. In fact, to the best of our knowledge, there is no authentication mechanism for WSNs in distributed IoT infrastructure has been proposed, which can support the properties such as anonymity, untraceability, etc. Nevertheless, the protocols presented in [14] and [18], all the sensor nodes share

TABLE II
PERFORMANCE BENCHMARKING BASED ON THE SECURITY PROPERTIES

Scheme	SP1	SP2	SP3	SP4	SP5
Kothmayr et al. [14]	No	No	No	No	No
Porambage et al. [18]	Yes	No	No	Yes	No
Proposed Scheme	Yes	Yes	Yes	Yes	Yes

SP: Security Property; **SP1:** Mutual Authentication; **SP2:** Anonymity; **SR3:** Untraceability; **SR4:** Resistance to Forgery Attacks; **SR5:** Resistance to Cloning Attacks;

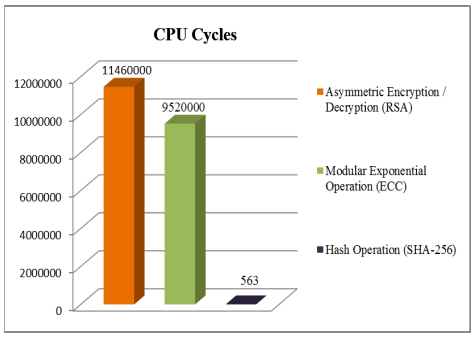


Fig. 4. Computational overhead of various cryptographic operations in terms of CPU cycles.

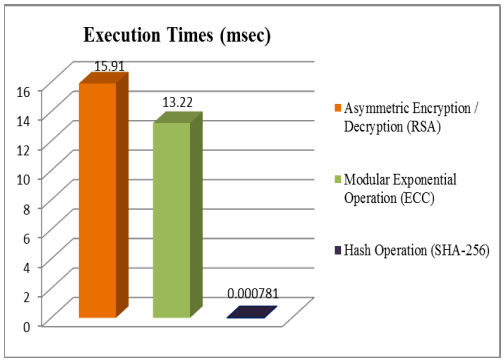


Fig. 5. Computational overhead of various cryptographic operations in terms of execution time.

a common key to communicate with their gateway. Because of that these protocols are vulnerable to cloning attacks and forgery attacks. Now, in order to analyze the performance of the proposed anonymous authentication scheme based on the computational overhead, here we simulate the hash operations, used in our proposed scheme and simultaneously, the other cryptographic operations adopted by the schemes presented in [14] and [18], by using CryptoPP library [29] on an Arm Cortex-A8 machine with the frequency 0.72 GHZ. Now, based on the simulation outcomes (shown in Fig. 4 and Fig. 5), asymmetric crypto-system RSA used in [14], takes 11.46×10^6 CPU cycles per operation with the execution time of 15.91 msec. On the other hand, each modular exponential operation in elliptic curve crypto system (ECC) used in [18], causes 9.52×10^6 CPU cycles with the execution time of 13.22 msec. We adopt SHA-256 for our proposed anonymous authentication scheme, where each hash operation (SHA-256) takes only 5.63×10^2 CPU cycles with the execution time of 0.00078 msec. In should be noted that, execution of our proposed scheme causes only 12 hash operations (maximum), where we neglect the execution time for each XOR operation. Therefore, execution our posed scheme causes 67.56×10^2 CPU cycles with the execution time of 0.0093 msec, which is significantly less than the CPU cycles and the execution time requires for each asymmetric operation in RSA and each modular exponential operation in ECC. Conclusively, performance of the proposed scheme in terms of the security, computational overhead, is better than these two recently proposed authentication schemes for WSNs in distributed IoT infrastructure. Hence, our proposed scheme is more suitable especially for the tiny-powered sensor node in distributed IoT applications.

VII. PROTOCOL ANALYSIS

In order to find out flaws in the proposed scheme, here we introduce formal analysis using BAN logic, which is basically a model logic with primitives which describe the belief of the principle involved in a crypto system. Using the inference rules of the BAN logic, authentication issues between the principles can be dealt with.

A. BAN Logic and Its Improvement

Three sorts of objects below are included in BAN logic [30]: principle, encryption keys and logical formulas. The main construction of BAN logic is described as follows. $P| \equiv X$ denotes P believes X; $P \Delta X$denotes that P sees X; $P| \sim X$ denotes that P said X; $P| \Rightarrow X$ denotes that P has jurisdiction over X; #(X) denotes that the formula X is fresh, that is X has not been sent in a message at any time before the current execution of the protocol. $P \overset{K}{\longleftrightarrow} Q$ denotes P and Q may use the shared K to communicate; $P \ni X$ denotes that P processes or is capable of processing, formula X; $\{X\}E_K$ denotes that the formula X is encrypted or encoded under the key K. The inference rules of BAN logic that are required in the analysis are described below.

1) Message-meaning rules R1: $\frac{P| \equiv P \leftrightarrow Q,\ P \Delta \{X\}E_K}{P| \equiv Q| \sim X}$;

2) Nonce-verification rules R2: $\frac{P|\equiv\#(X),\ P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$;
3) Jurisdiction rules R3: $\frac{P|\equiv Q|\Rightarrow X,\ P|\equiv Q|\equiv X}{P|\equiv X}$;
4) Seeing rules R4 : $\frac{P\,\Delta(X,Y)}{P\,\Delta X}$; R5 : $\frac{P|\equiv P\overset{K}{\longleftrightarrow}Q,\ P\,\Delta\{X\}E_K}{P\,\Delta X}$;
5) Fresh rules R6: $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$;
6) Belief rules R7: $\frac{P|\equiv(X,Y)}{P|\equiv X}$;

Now, in order to analyze the properties of our proposed scheme, here we need to extend the BAN logic with the following: ER1: $\frac{P|\equiv Q\overset{K}{\longleftrightarrow}P,P\,\Delta f(X,Y)}{P|\equiv Q|\sim X}$, where the extension rule ER1 denotes that the key K is shared among P and Q; function f is used to verify the originality of the principles.

B. Formal Analysis of the Proposed Scheme

The initial security assumptions about Sensor node (Sn), Cluster Head (CH), and HIoTS (H) are as follows:

$$1.\ \mathrm{Sn}|\equiv \mathrm{H}\overset{K_{sh}}{\longleftrightarrow}\mathrm{Sn};\quad 2.\ \mathrm{H}|\equiv \mathrm{Sn}\overset{K_{sh}}{\longleftrightarrow}\mathrm{H};$$
$$3.\ \mathrm{CH}|\equiv \mathrm{H}\overset{K_{ch}}{\longleftrightarrow}\mathrm{CH};\quad 4.\ \mathrm{H}|\equiv \mathrm{CH}\overset{K_{ch}}{\longleftrightarrow}\mathrm{H};$$

In our proposed scheme, HIOTS believes the legitimacy of the sensor node (Sn) with the help of one-time alias identity AID_{Sn} i.e. $\mathrm{H}|\equiv \mathrm{Sn}|\sim\{AID_{Sn}\}$. Therefore, by expending the principle ER1, we can derive the following statement:

$$\frac{\mathrm{H}|\equiv \mathrm{Sn}\overset{K_{sh}}{\longleftrightarrow}\mathrm{H},\ \mathrm{H}\,\Delta f(h(ID_{Sn_i}\|K_{sh}\|N_s\|Tr_{seq}),AID_{Sn})}{\mathrm{H}|\equiv \mathrm{Sn}|\sim AID_{Sn}}$$

Moreover, by utilizing the principles R7 and R6 we can also establish the following statements for HIoTS (H):

$$\frac{\mathrm{H}|\equiv(N_s,AID_{Sn})}{\mathrm{H}|\equiv N_s};\quad \frac{\mathrm{H}|\equiv\#(Tr_{seq})}{\mathrm{H}\equiv\#(Tr_{seq},AID_{Sn})}$$
$$\text{and}\ \ \frac{\mathrm{H}|\equiv\#(Tr_{seq})}{\mathrm{H}|\equiv\#(Tr_{seq},N_s)}.$$

In our proposed scheme, HIOTS (S) authenticates the Cluster Head (CH) by using the parameter V_2, i.e. $\mathrm{H}|\equiv \mathrm{CH}|\sim\{V_2\}$, more accurately, by employing the principle ER1, we can derive the following statement: $\frac{\mathrm{H}|\equiv\mathrm{CH}\overset{K_{ch}}{\longleftrightarrow}\mathrm{H},\ \mathrm{H}\,\Delta f(h(\mathrm{M_{A_1}}\|N_c\|K_{ch}),V_2)}{\mathrm{H}|\equiv\mathrm{CH}|\sim V_2}$; and based on that we can establish the following:

$$\frac{\mathrm{H}|\ \equiv\ (\mathrm{M_{A_2}},V_2)}{\mathrm{H}|\equiv\mathrm{M_{A_2}}};\quad \frac{\mathrm{H}|\equiv\#(Tr_{Seq})}{\mathrm{H}|\equiv\#(Tr_{Seq},\mathrm{M_{A_2}})}.$$

Now, the Cluster Head (CH) believes the trustworthiness of the HIoTS (H) based on the value of the parameter V_3 in

$$\mathrm{M_{A_3}}\ \text{i.e.}\ \mathrm{CH}|\equiv\mathrm{H}|\sim\mathrm{M_{A_3}},\quad \exists\ \mathrm{CH}|\equiv\#(V_3)$$
$$\text{and}\ \frac{\mathrm{CH}|\equiv(\mathrm{M_{A_3}},V_3)}{\mathrm{CH}|\equiv\mathrm{M_{A_3}}};$$

More precisely, by applying the principle ER1 we can write,

$$\frac{\mathrm{CH}|\equiv \mathrm{H}\overset{K_{ch}}{\longleftrightarrow}\mathrm{CH},\ \mathrm{CH}\ \Delta f(h(ID_{Ch_j}\|N_c\|K_{ch}),V_3)}{\mathrm{CH}|\equiv \mathrm{H}|\sim V_3};$$

and simultaneously by expending the principles R6 and R3 we can also constitute the following statements:

$$\frac{\mathrm{CH}|\equiv\#(N_c)}{\mathrm{CH}|\equiv\#(N_c,V_3)};\quad \frac{\mathrm{CH}|\equiv\#(V_3)}{\mathrm{CH}|\equiv\#(V_3,\mathrm{M_{A_3}})};$$
$$\frac{\mathrm{CH}\ |\equiv\ \mathrm{H}|\Rightarrow V_3,\mathrm{CH}|\equiv\ \mathrm{H}\ \equiv V_3}{\mathrm{CH}|\equiv V_3};$$

Now, for the sensor node (Sn), which believes the trustworthiness of the HIoTS (H) based on the value of the parameter V_4 in $\mathrm{M_{A_4}}$ i.e. $\mathrm{Sn}|\equiv\ \mathrm{H}|\sim\ \mathrm{M_{A_4}},\exists\ \mathrm{Sn}|\equiv\#(V_4)$; and $\frac{\mathrm{Sn}|\equiv(\mathrm{M_{A_4}},V_4)}{\mathrm{Sn}\,|\equiv\mathrm{M_{A_4}}}$; precisely, by expending the principle ER1, we can make the following declaration:

$$\frac{\mathrm{Sn}|\equiv \mathrm{H}\overset{K_{sh}}{\longleftrightarrow}\mathrm{Sn},\ \mathrm{Sn}\ \Delta f(h(Tr\|K_{sh}\|ID_{Sn_i}),V_4)}{\mathrm{Sn}|\equiv \mathrm{H}|\sim V_4}.$$

Besides, the sensor Sn can verify the parameter Tr, which is imperative for the most recent $Tr_{seq_{new}}$. Since in case of wrong Tr, Sn will form the wrong track sequence number. In that case using the principle R7, we can constitute the following statements: $\frac{\mathrm{Sn}|\equiv(Tr,V_4)}{\mathrm{Sn}|\equiv Tr}$; $\frac{\mathrm{Sn}|\equiv(Tr_{seq_{new}},Tr)}{\mathrm{Sn}\,|\equiv Tr}$; where $Tr=h(K_{sh}\|ID_{Sn_i}\|N_s)\oplus Tr_{seq_{new}}$.

In this way, the Sensor node (Sn), Cluster Head (CH), and HIoTS (H) can authenticate themselves through the legitimate security capabilities. Now, from the above analysis using the BAN logic, we have proved that the protocol used in the proposed scheme is correct where the legitimate participants (Sn, CH, and H) can authenticate each other by using the several security capabilities, if the executions of the protocols are successful.

VIII. Conclusion

In this article, at first we have introduced a distributed IoT system architecture and subsequently we have also introduced and analyzed an authentication mechanism for WSNs in distributed IoT applications. The proposed authentication scheme comprises of three phases: registration phase for obtaining cryptographic credentials by a sensor node, inter-cluster movement phase, where a sensor node remains in the same WSN but can move from one cluster to another by preserving strong anonymity, and inter-network movement phase for secure inter-network movement of the sensor node. In comparison with existing schemes, our proposed scheme provides more security features with the assurance of less computational overhead. Accordingly, our proposed scheme is suitable for the resource-constrained WSN based IoT system.

Acknowledgments

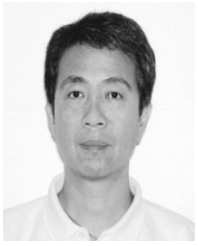
The authors would like to thank the Ministry of Science and Technology, Taiwan, for their benign supports. The authors also would like to thank the editor and all the anonymous referees for their valuable suggestions.

References

[1] *IBM: A Smarter Planet*. [Online]. Available: http://www.ibm.com/smarterplanet/, accessed Oct. 2010.
[2] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, *Transmission of IPv6 Packets Over IEEE 802.15.4 Networks*, RFC 4944, 2007.

[3] D. Guinard, M. Fischer, and V. Trifa, "Sharing using social networks in a composable Web of Things," in *Proc. 8th IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOM Workshops)*, Mar./Apr. 2010, pp. 702–707.
[4] *Libelium: Interfacing the Sensor Networks With the Web 2.0*. [Online]. Available: http://www.libelium.com/, accessed Oct. 2010.
[5] C. P. Mayer, "Security and privacy challenges in the Internet of Things," in *Proc. KiVS Workshop Global Sensor Netw.*, 2009, pp. 1–12.
[6] J. Claessens, "Trust, security, privacy, and identity perspective," in *Panel on Future Internet Service Offer*. 2008.
[7] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 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, no. 4, pp. 612–619, Dec. 2014.
[10] Y. Liu, J. Li, and M. Guizani, "PKC based broadcast authentication using signature amortization for WSNs," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2106–2115, Jun. 2012.
[11] T. Kwon and J. Hong, "Secure and efficient broadcast authentication in wireless sensor networks," *IEEE Trans. Comput.*, vol. 59, no. 8, pp. 1120–1133, Aug. 2010.
[12] E. Rescorla and N. Modadugu, *Datagram Transport Layer Security,* document IETF RFC 4347, Apr. 2006. [Online]. Available: http://tools.ietf.org/html/rfc4347
[13] Z. Shelby, K. Hartke, and C. Bormann, *Constrained Application Protocol (CoAP)*, IETF RFC 7252, 2013. [Online]. Available: http://tools.ietf.org/pdf/draft-ietf-core-coap-18.pdf
[14] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2710–2723, Nov. 2013.
[15] X. H. Le *et al.*, "An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography," *J. Commun. Netw.*, vol. 11, no. 6, pp. 599–606, Dec. 2009.
[16] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks," *Int. J. Innovative Comput., Inf. Control*, vol. 5, no. 8, pp. 2107–2124, 2009.
[17] P. Kotzanikolaou and E. Magkos, "Hybrid key establishment for multiphase self-organized sensor networks," in *Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, Jun. 2005, pp. 581–587.
[18] 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. Sensor Netw.*, vol. 2014, Jul. 2014, Art. ID 357430.
[19] C. H. Wang and C. Y. Lin, "An efficient delegation-based roaming payment protocol against denial of service attacks," in *Proc. Int. Conf. Electron., Commun. Control*, Sep. 2011, pp. 4136–4140.
[20] T. Hwang and P. Gope, "Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets," *Wireless Pers. Commun.*, vol. 77, no. 1, pp. 197–224, Jul. 2014.
[21] P. Gope and T. Hwang, "Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks," *Wireless Pers. Commun.*, vol. 82, no. 4, pp. 2231–2245, Jun. 2015.
[22] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID," in *Proc. Workshop RFID Lightweight Cryptograph.*, 2005, pp. 17–24.
[23] C. Qingling, Z. Yiju, and W. Yonghua, "A minimalist mutual authentication protocol for RFID system & BAN logic analysis," in *Proc. ISECS Int. Colloq. Comput., Commun., Control, Manage.*, Aug. 2008, pp. 449–453.
[24] Z. Luo, T. Chan, and J. S. Li, "A lightweight mutual authentication protocol for RFID networks," in *Proc. IEEE Int. Conf. e-Bus. Eng. (ICEBE)*, Oct. 2005, pp. 620–625.
[25] C. C. Tan, B. Sheng, and Q. Li, "Secure and serverless RFID authentication and search protocols," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1400–1407, Apr. 2008.
[26] S. Cai, Y. Li, T. Li, and R. H. Deng, "Attacks and improvements to an RIFD mutual authentication protocol and its extensions," in *Proc. 2nd ACM Conf. Wireless Netw. Secur. (WiSec)*, 2009, pp. 51–58.
[27] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," *Comput. Secur.*, doi: 10.1016/j.cose.2015.05.004,2015.
[28] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Syst. J.*, 2015, doi: 10.1109/JSYST.2015.2416396.
[29] *Crypto++ Library*. [Online]. Available: http://www.cryptopp.com, accessed Jan. 25, 2015.
[30] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

Prosanta Gope received the M.Tech. degree in computer science and engineering from the National Institute of Technology, Durgapur, India, in 2009. He is currently pursuing the Ph.D. degree in computer science and information engineering at National Cheng Kung University, Tainan, Taiwan. His research interests include authentication, authenticated encryption, access control system, security in mobile communication, and cloud computing.



Tzonelih Hwang received the M.S. and Ph.D. degrees in computer science from the University of Southwestern Louisiana, USA, in 1988. He is currently a Distinguished Professor with the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan. He has actively participated in several research activities, including as a Research Scientist with the Center for Advanced Computer Studies, University of Southwestern Louisiana. He is also a Vigorous Member of the Editorial Board of some reputable international journals. He has authored over 250 technical papers and holds five patents. His research interests include network and information security, access control systems, error control codes, security in mobile communication, and quantum cryptography.