Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things

Huansheng Ning, *Senior Member, IEEE*, Hong Liu, *Student Member, IEEE*, and Laurence T. Yang, *Member, IEEE*

Abstract—The Internet of Things (IoT) is becoming an attractive system paradigm to realize interconnections through the physical, cyber, and social spaces. During the interactions among the ubiquitous things, security issues become noteworthy, and it is significant to establish enhanced solutions for security protection. In this work, we focus on an existing U2IoT architecture (i.e., unit IoT and ubiquitous IoT), to design an aggregated-proof based hierarchical authentication scheme (APHA) for the layered networks. Concretely, 1) the aggregated-proofs are established for multiple targets to achieve backward and forward anonymous data transmission; 2) the directed path descriptors, homomorphism functions, and Chebyshev chaotic maps are jointly applied for mutual authentication; 3) different access authorities are assigned to achieve hierarchical access control. Meanwhile, the BAN logic formal analysis is performed to prove that the proposed APHA has no obvious security defects, and it is potentially available for the U2IoT architecture and other IoT applications.

Index Terms—Internet of Things (IoT), authentication protocol, security, U2IoT architecture

1 Introduction

The Internet of Things (IoT) is emerging as an attractive system paradigm to integrate physical perceptions, cyber interactions, and social correlations, in which the physical objects, cyber entities, and social attributes are required to achieve interconnections with the embedded intelligence [1]. During the interconnections, the IoT is suffering from severe security challenges, and there are potential vulnerabilities due to the complicated networks referring to heterogeneous targets, sensors, and backend management systems [2]. It becomes noteworthy to address the security issues for the ubiquitous things in the IoT.

Recent studies have been worked on the general IoT, including system models, service platforms, infrastructure architectures, and standardization. Particularly, a human-society inspired U2IoT architecture (i.e., unit IoT and ubiquitous IoT) is proposed to achieve the physical-cyber-social convergence (as shown in Fig. 1) [3]. In the U2IoT architecture, mankind neural system and social organization framework are introduced to establish the single-application and multi-application IoT frameworks. Multiple unit IoTs compose a local IoT within a region, or an industrial IoT for an industry. The local IoTs and industrial IoTs are covered within a national IoT, and jointly form the ubiquitous IoT.

Towards the IoT security, related works mainly refer to the security architectures and recommended countermeasures [4], [5], [6], [7], [8], secure communication and networking mechanisms [9], [10], [11], [12], [13], cryptography algorithms [14], [15], [16], [17], [18], [19], and application security solutions [20], [21], [22]. Current researches mainly refer to three aspects: system security, network security, and application security.

- *System security* mainly considers a whole IoT system to identify the unique security and privacy challenges, to design systemic security frameworks, and to provide security measures and guidelines.
- *Network security* mainly focuses on wireless communication networks (e.g., wireless sensor networks (WSN), radio frequency identification (RFID), and the Internet) to design key distribution algorithms, authentication protocols, advanced signature algorithms, access control mechanisms, and secure routing protocols. Particularly, authentication protocols are popular to address security and privacy issues in the IoT, and should be designed considering the things' heterogeneity and hierarchy.
- *Application security* serves for IoT applications (e.g., multimedia, smart home, and smart grid), and resolves practical problems with particular scenario requirements.

However, the existing security solutions mainly provide security approaches for a general IoT, and there is little authentication scheme particularly designed for the U2IoT architecture. It becomes necessary to establish an authentication scheme to realize its security protection. In this work, the main purpose is to provide bottom-up

- *H. Ning is with the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China, and also with the School of Electronic and Information Engineering, Beihang University, Beijing, China. E-mail: ninghuansheng@ustb.edu.cn.*
- *H. Liu is with the School of Electronic and Information Engineering, Beihang University, Beijing, China. E-mail: liuhongler@ee.buaa.edu.cn.*
- *L.T. Yang is with the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, HuBei, China, and also with the Department of Computer Science, St. Francis Xavier University, Antigonish, Canada. E-mail: ltyang@stfx.ca.*

Manuscript received 30 Oct. 2013; revised 17 Jan. 2014; accepted 28 Feb. 2014. Date of publication 13 Mar. 2014; date of current version 6 Feb. 2015. Recommended for acceptance by G. Wang.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TPDS.2014.2311791

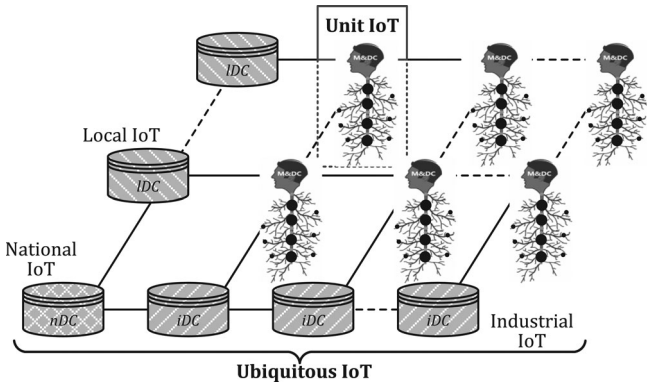

Fig. 1. The U2IoT architecture.

safeguard for the U2IoT architecture to realize secure interactions.

Towards the U2IoT architecture, a reasonable authentication scheme should satisfy the following requirements. *1) Data CIA* (i.e., *confidentiality, integrity, and availability):* The exchanged messages between any two legal entities should be protected against illegal access and modification. The communication channels should be reliable for the legal entities. *2) Hierarchical access control:* Diverse access authorities are assigned to different entities to provide hierarchical interactions. An unauthorised entity cannot access data exceeding its permission. *3) Forward security:* Attackers cannot correlate any two communication sessions, and also cannot derive the previous interrogations according to the ongoing session. *4) Mutual authentication:* The untrusted entities should pass each other's verification so that only the legal entity can access the networks for data acquisition. *5) Privacy preservation:* The sensors cannot correlate or disclose an individual target's private information (e.g., location). Considering above security requirements, we design an aggregated-proof based hierarchical authentication scheme (APHA) for the unit IoT and ubiquitous IoT respectively, and the main contributions are as follows:

1) Aggregated-proofs are established by wrapping multiple targets' messages for anonymous data transmission, which realizes that individual information cannot be revealed during both backward and forward communication channels,
2) Directed path descriptors are defined based on homomorphism functions to establish correlation during the cross-layer interactions. Chebyshev chaotic maps are applied to describe the mapping relationships between the shared secrets and the path descriptors for mutual authentication,
3) Diverse access authorities on the group identifiers and pseudonyms are assigned to different entities for achieving the hierarchical access control through the layered networks.

The remainder of the paper is organized as follows. Section 2 reviews the related work in the IoT security. Section 3 presents the layered system model, and introduces the proposed authentication scheme. Section 4 introduces the BAN logic based formal analysis. Finally, Section 5 draws a conclusion.

2 Related Work

2.1 System Security

Roman et al. [4] pointed out that the traditional security mechanisms may not be competent for the heterogeneous networks, therefore improved mechanisms should be designed according to the IoT infrastructures. Particularly, the authors introduced cryptology based guidance to address the security challenges, referring to the identity management, trust governance frameworks, fault tolerance, cryptography protocol, identity ownership, and privacy preservation.

Lampropoulos and Denazis [5] focused on the identity management in future Internet to analyze the identification and authentication issues in the user-centric, federations, and other orthogonal systems. Furthermore, a distributed dynamic identity mapping, association N' discovery system (DIMANDS) was established to achieve cross-federation service delivery, and to authenticate an unknown entity in a foreign network and online service payment. The proposed DIMANDS can achieve trusted and secure associations in heterogeneous contexts.

Heer et al. [6] considered IP-based IoT, discussed the applicability and limitations of current Internet protocols, and presented a thing lifecycle based security architecture for the IP networks. Thereinto, security architecture, node security model, and security bootstrapping are considered in the security solution. Moreover, the authors pointed that the security protocols should fully consider the resource-constrained heterogeneous communication environments. Meca et al. [7] proposed a security architecture based on the host identity protocol (HIP) and multimedia Internet keying protocols to enhance secure network association and key management.

Ning et al. [8] addressed the cyber-entity security to present the recommended security approaches according to a cyber-entity's activity cycle, and further established a secure interaction solution for three scenarios (i.e., secure data access interaction, privacy-preserving data sharing interaction, and secure access authority transfer interaction).

2.2 Network Security

Hancke et al. [9] identified the security challenges for the user-oriented RFID systems in the IoT, and the major challenges (e.g., privacy, ownership, data integrity, application integrity, and security standardization) should be enhanced to achieve universal security. Yan and Wen [10] applied a mobile RFID security protocol to guarantee the mobile RFID networks, and a trust third party (TTP) based key management protocol is introduced to construct a secure session key. Toumi et al. [11] focused on the integration of RFID tags into IP networks, and proposed a HIP address translation scheme. The scheme provides address translation services between the tag identifiers and IP addresses, which presents a prototype of the cross-layer IoT networks. Chang and Chen [12] reviewed the trust-based mechanisms (e.g., cryptographic, and authentication) in WSNs. Raza et al. [13] presented Lithe, which is an integration of datagram transport layer security (DTLS) and constrained application protocol (CoAP) to protect the transmission of sensitive information in the IoT.

TABLE 1
The Shared Secrets Distribution

	T_j	R_b	DC_a	iDC	nDC
gid_{T_j}	√	√	√	×	×
gid_{S_b}	√	√	√	×	×
gid_{DC_a}	×	×	√	×	×
gid_{iDC}	×	×	√	√	√
PID_{T_j}	√	×	√	×	×
PID_{S_b}	×	√	√	×	×
PID_{DC_a}	×	×	√	√	√
PID_{iDC}	×	×	×	√	×

√: The secret is available; ×: The secret is unavailable.

Yao et al. [14] revised Nyberg's fast one-way accumulator to design a message authentication code (MAC) based multicast authentication mechanism for small-scale IoT applications. Roman et al. [15] considered WSNs to provide key management mechanisms to allow that two remote devices can negotiate certain security certificates (e.g., shared keys, Blom key pairs, and polynomial shares). The authors analyzed the applicability of existing mechanisms, including public key infrastructure (PKI) and pre-shared keys for sensor nodes in IoT contexts. Ren and Ma [16] proposed an attribute-based access control model according to bilinear mappings. The scheme realizes anonymous access, and minimizes the number of the exchanged messages in the open channels. Chen et al. [17] proposed a fuzzy reputation based trust management model (TRM-IoT) to enforce the entities' cooperation and interconnection. Wang et al. [18] proposed an anonymous authentication protocol, and applied the pseudonym and threshold secret sharing mechanism to achieve the tradeoff between anonymity and certification. Zhao et al. [19] proposed a mutual authentication scheme, which is designed based on the feature extraction, secure hash algorithm (SHA), and elliptic curve cryptography (ECC). Thereinto, asymmetric authentication scheme is established without compromising computation cost and communication overhead.

2.3 Application Security

Zhou and Chao [20] established a media-aware traffic security architecture for the IoT, and the architecture is based on the current traffic classification to enable the heterogeneous multimedia services becoming available in real-time mode. Concretely, key management, batch rekeying, authentication, watermarking, and distributed secret sharing are introduced into the security architecture.

Li et al. [21] established a smart community model for IoT applications, and a cyber-physical system with the networked smart homes was introduced with security considerations. Filtering false network traffic and avoiding unreliable home gateways are suggested for safeguard. Meanwhile, the security challenges are discussed, including the cooperative authentication, unreliable node detection, target tracking, and intrusion detection.

Sridhar et al. [22] analyzed cyber infrastructure security in the smart grid. A layered security scheme was established to evaluate security risks for the power applications. The authors highlighted power generation, transmission, distribution control and security, and introduced encryption, authentication, and access control to achieve secure communications. Furthermore, digital forensics, security incident and event management are applied for management, and cyber-security evaluation and intrusion tolerance are also considered.

TABLE 2
Notations

Notation	Description
nDC	The national data center.
iDC	The industrial data center.
DC_a	The a-th unit data center within iDC's jurisdiction.
S_b, T_j	The b-th sensor, and the j-th target within DC_a's jurisdiction.
F	The pseudo-random identify flag.
gid, PID	The pseudo group identifier, and pseudonym.
M^{ℓ}, M'	The locally re-computed, and the updated value.
p_y^x	The directed path descriptor pointing from E_y to E_x, in which $\{E_x, E_y\}$ represent entities, and $\{x, y\}$ are the entities' identity labels.
p_{ym}^{mx}	The path descriptor owned by a media entity E_m.
$\lvert p_{ym}^{mx} \rvert$	The mirroring path descriptor computed by E_m.
r	The pseudo-random number.
k_a, k_n	The authentication keys shared by $\{iDC, DC_a\}$ and $\{iDC, nDC\}$.
$\mathcal{H}(.)$, $\mathcal{H}_*(.)$	The hash function, and hash based message authentication code (HMAC) function.
$\mathcal{E}(.)$	The encryption.
$\mathcal{F}(.)$, $\mathcal{T}_*(.)$	The homomorphism function, and Chebyshev polynomial.
Ξ, Σ	The multi-element cascade, and summation.

3 The Authentication Scheme: APHA

3.1 System Initialization

In the U2IoT architecture, the unit IoT refers to a basic network unit for a single application, and the ubiquitous IoT includes multiple applications within the centralized national management [3]. Here, we consider an industry-oriented scenario, in which multiple industrial IoTs manage the corresponding unit IoTs in diverse industries (e.g., smart grid). Meanwhile, the industrial IoTs are under the jurisdiction of a national IoT to realize interconnections. In the system model, there are heterogeneous sensors (S) and targets (T), which are various according to different scenarios. Multiple unit data centers (DC) are under a particular industrial IoT's jurisdiction, and industrial data centers (iDC) have relatively independent authorities on a certain DC. Meanwhile, the trusted national data center (nDC) is introduced to manage multiple iDCs.

Here, we consider $\{T_j, S_b, DC_a\}$ $(j = \{1, \ldots, J\})$ in the unit IoT, and $\{DC_a, iDC, nDC\}$ in the ubiquitous IoT. Each entity stores its assigned group identifiers and pseudonyms, as shown in Table 1. Meanwhile, the directed path descriptors are introduced as authentication operators, and owned by the subscript labeled entity to point to the superscript labeled entity. It means that p_y^x is owned by E_y, and represents the path descriptor pointing from E_y to E_x. The detailed notations are introduced in Table 2.

The APHA is designed based on two main cryptographic primitives: a homomorphism function $\mathcal{F}(.)$, and Chebyshev polynomials $\mathcal{T}_*(.)$.

- *Towards the homomorphism function.*

According to Fermat's Little theorem: If q is a prime number, and x is not a multiple of q, thus $x^{q-1} \equiv 1 \bmod q$.

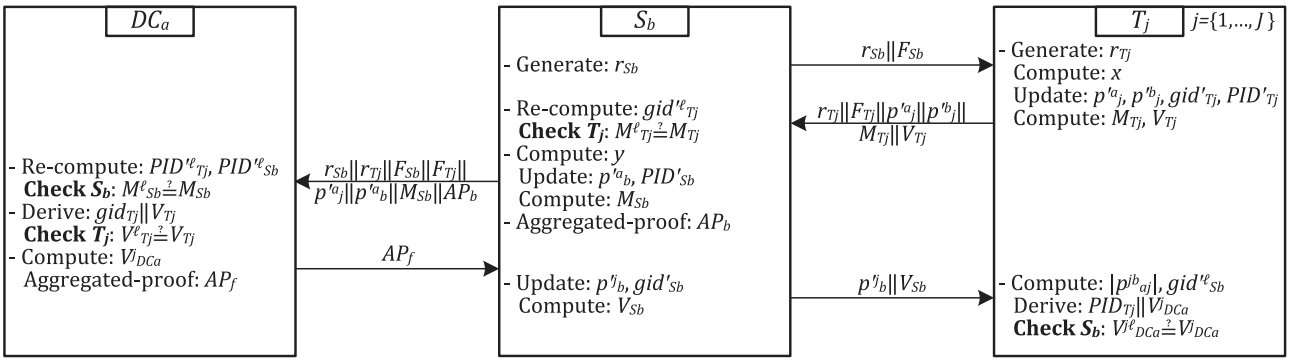

Fig. 2. The authentication protocol in the unit IoT.

A homomorphism encryption algorithm can be designed as follows [23].

1) Choose two large prime numbers p and q. and let $n = pq$, in which n is a public number, and p and q are private numbers.
2) A real number x is in a plaintext with the effective decimal digits d for $g_1(x) = 10^d x$. Here, $|g_1(x)| \leq (p-1)/2$, and $g_2(g_1(x)) \in \mathbb{Z}_p$. Define a homomorphism function $\mathcal{F} : \mathcal{F}(x) = g_2(g_1(x))^{k(p-1)+1} \bmod n = C$.
3) The inverse operation $\mathcal{F}^{-1}(.)$ satisfies that: $\mathcal{F}^{-1}(\mathcal{F}(x)) = g_2^{-1}(c \bmod p)/10^d = x$.

For $\{x, y\} \in \mathbb{R}$ and $\{g_1(x), g_1(y)\} \leq (p-1)/4$, $\mathcal{F}(x+y) = \mathcal{F}(x) + \mathcal{F}(y)$ holds. Similarly, for $\{x, y\} \in \mathbb{R}$ and $\{g_1(x), g_1(y)\} \leq \sqrt{(p-1)/2}, \mathcal{F}(xy) = \mathcal{F}(x)\mathcal{F}(y)$ holds.

The homomorphism function $\mathcal{F}(.)$ is applied to describe the relationships of the directed path descriptors. For instance, the pairwise path descriptors $\{p_j^b, p_b^j\}$ are respectively owned by $\{T_j, S_b\}$, and satisfy the following relationships, in which the secrets C_j^b and C_b^j are owned by $\{T_j, S_b\}$ for $C_j^b = C_b^j \in \mathbb{R}^*$. Here, T_j can obtain a mirroring path descriptor $|p_{aj}^{jb}|$, which equals $p_{aj}^{jb} \oplus PID_{T_j}$.

$$\mathcal{F}(p_j^b p_b^j) = \mathcal{F}(p_j^b)\mathcal{F}(p_b^j) = C_j^b = C_b^j,$$
$$\mathcal{F}(p_a^j + p_j^b) = \mathcal{F}(p_a^j) + \mathcal{F}(p_j^b) = \mathcal{F}(|p_{aj}^{jb}|).$$

- *Towards the Chebyshev polynomials.*

The Chebyshev chaotic maps can be applied for authentication [24], [25]. Assume that $\mathcal{T}_l(m)$ is a Chebyshev polynomial in l of degree m, and $\mathcal{T}_l(m) : [-1, 1] \rightarrow [-1, 1]$ is defined as $\mathcal{T}_l(m) = \cos(l \cdot \arccos(m))$. The recurrence relationships of Chebyshev polynomials are as follows:

$$\mathcal{T}_0(m) = 1, \qquad \mathcal{T}_1(m) = m,$$
$$\mathcal{T}_l(m) = \cos(l \cdot \arccos(m)); \quad (l \geq 2).$$

Let the degrees $\{l_1, l_2\}$ be positive integer numbers. The Chebyshev polynomials $\mathcal{T}_{l_1}(m)$ and $\mathcal{T}_{l_2}(m)$ $(m \in [-\infty, \infty])$ satisfy the semigroup and chaotic properties:

$$\mathcal{T}_l(m) \equiv (2m\mathcal{T}_{l-1}(m) - \mathcal{T}_{l-2}(m)) \pmod q; \quad (l \geq 2),$$
$$\mathcal{T}_{l_1}(\mathcal{T}_{l_2}(m)) \equiv \mathcal{T}_{l_1 l_2}(m) \equiv \mathcal{T}_{l_2}(\mathcal{T}_{l_1}(m)) \pmod q.$$

Accordingly, a set of Chebyshev polynomials are assigned to represent the relationships of the group identifiers/pseudonyms and directed path descriptors:

$$\begin{aligned}
&\text{For } \mathcal{T}_{l_{T_j}}(.): && gid_{S_b} \equiv \mathcal{T}_{l_{T_j}}(\mathcal{F}(p_j^b)) \pmod q,\\
&\text{For } \mathcal{T}_{l_{S_b}}(.): && gid_{T_j} \equiv \mathcal{T}_{l_{S_b}}(\mathcal{F}(p_b^j)) \pmod q,\\
&\text{For } \mathcal{T}_{l_{DC_a}}(.): && PID_{T_j} \equiv \mathcal{T}_{l_{DC_a}}(\mathcal{F}(p_a^j)) \pmod q,\\
& && PID_{S_b} \equiv \mathcal{T}_{l_{DC_a}}(\mathcal{F}(p_a^b)) \pmod q,\\
& && gid_{iDC} \equiv \mathcal{T}_{l_{DC_a}}(\mathcal{F}(p_a^i)) \pmod q,\\
&\text{For } \mathcal{T}_{l_{iDC}}(.): && PID_{DC_a} \equiv \mathcal{T}_{l_{iDC}}(\mathcal{F}(p_i^a)) \pmod q,\\
&\text{For } \mathcal{T}_{l_{nDC}}(.): && gid_{DC_a} \equiv \mathcal{T}_{l_{nDC}}(\mathcal{F}(p_n^a)) \pmod q,\\
& && PID_{iDC} \equiv \mathcal{T}_{l_{nDC}}(\mathcal{F}(p_n^i)) \pmod q.
\end{aligned}$$

Besides, the group identifiers $\{gid_{iDC}, gid_{DC_a}\}$ can be respectively extended into $\{gid_{iDC}^n\}$ (i.e., $\{gid_{iDC}^1, \ldots, gid_{iDC}^{N_1}\}$) and $\{gid_{DC_a}^n\}$ (i.e., $\{gid_{DC_a}^1, \ldots, gid_{DC_a}^{N_2}\}$) for $\{N_1, N_2\} \in \mathbb{N}^*$ and $\{gid_{iDC}^n, gid_{DC_a}^n\} \in \mathbb{Z}_{q^2}^*$. There are the following relationships for $x \in \{iDC, DC_a\}$ and $y \in \{\eta_{DC_a}, \varphi_{nDC}\}$:

$$PID_x \equiv \prod_{n=1}^{N_2} (y)^{gid_x^n} \pmod{q^2}.$$

In the trust model, nDC is an only entity trusted by all the other entities (i.e., T_j, S_b, DC_a, iDC). In the unit IoT, DC_a is trusted by $\{T_j, S_b\}$, and is under iDC's default jurisdiction. In the ubiquitous IoT, iDC and nDC have relatively independent jurisdictions on DC_a.

3.2 The Authentication Protocol in the Unit IoT

Fig. 2 shows an interaction among $\{DC_a, S_b, T_j\}$, in which T_j represents multiple targets $\{T_1, \ldots, T_J\}$.

3.2.1 Challenge-Response between S_b and T_j, and S_b's Verification on T_j

S_b generates a random number r_{S_b}, extracts its temp identity flag F_{S_b}, and transmits $r_{S_b} \| F_{S_b}$ to T_j as a challenge to initiate a new session. Upon receiving the messages, T_j first ascertains S_b's identity by searching the matched identity flag F_{S_b}, generates a random number r_{T_j}, and extracts a set of values $\{F_{T_j}, gid_{T_j}, PID_{T_j}, C_j^a, C_j^b, p_j^a, p_j^b\}$, in which $\{C_j^a, C_j^b\}$ are shared secrets, and $\{p_j^a, p_j^b\}$ are directed path descriptors. Thereafter, T_j computes a positive integer $x = [r_{S_b}] \pmod e$ for $e \in \mathbb{N}^*$ as the maximum degree of a

Chebyshev polynomial $\mathcal{T}_x(.)$. T_j updates $\{p_j^a, p_j^b, gid_{T_j}, PID_{T_j}\}$ into $\{p_j'^a, p_j'^b, gid'_{T_j}, PID'_{T_j}\}$:

$$\begin{aligned} p_j'^a &= \mathcal{T}_x\big(C_j^a/\mathcal{F}\big(p_j^a\big)\big) \pmod q,\\ p_j'^b &= \mathcal{T}_x\big(C_j^b/\mathcal{F}\big(p_j^b\big)\big) \pmod q,\\ gid'_{T_j} &= \mathcal{T}_x(gid_{T_j}) \pmod q,\\ PID'_{T_j} &= \mathcal{T}_x(PID_{T_j}) \pmod q\ . \end{aligned}$$

T_j computes M_{T_j} and V_{T_j}, in which M_{T_j} is an authentication operator, and V_{T_j} is further used to establish the backward aggregated-proof AP_b:

$$\begin{aligned} M_{T_j} &= \mathcal{H}\big(r_{S_b}\|gid'_{T_j}\big),\\ V_{T_j} &= \mathcal{H}\big(r_{T_j}\|PID'_{T_j}\big). \end{aligned}$$

T_j transmits $r_{T_j}\|F_{T_j}\|p_j'^a\|p_j'^b\|M_{T_j}\|V_{T_j}$ to S_b. Thereafter, S_b first ascertains T_j's identity by F_{T_j}, and locally re-computes $gid_{T_j}''^{\ell}$. Theoretically, $gid_{T_j}''^{\ell}$ equals gid'_{T_j} according to $gid_{T_j} \equiv \mathcal{T}_{l_{S_b}}(\mathcal{F}(p_b^j)) \pmod q$:

$$gid_{T_j}''^{\ell} = \mathcal{T}_{l_{S_b}}\big(p_j'^b\big) \pmod q.$$

S_b checks T_j by re-computing $M_{T_j}^{\ell} = \mathcal{H}(r_{S_b}\|gid_{T_j}''^{\ell})$. If $M_{T_j}^{\ell} = M_{T_j}$ holds, S_b will regard T_j as a legal target; otherwise, the APHA will terminate.

3.2.2 Backward Aggregated-Proof Challenge and DC_a's Verification on $\{T_j, S_b\}$

S_b extracts $\{gid_{T_j}, PID_{S_b}, C_b^a, p_b^a\}$, and computes a random integer $y = [r_{T_j}] \pmod e$ to denote the degree of the Chebyshev polynomial $\mathcal{T}_y(.)$. Afterwards, S_b obtains the updated values $\{p_b'^a, PID'_{S_b}\}$, and computes an authentication operator M_{S_b}:

$$\begin{aligned} p_b'^a &= \mathcal{T}_y\big(C_b^a/\mathcal{F}\big(p_b^a\big)\big) \pmod q,\\ PID'_{S_b} &= \mathcal{T}_y(PID_{S_b}) \pmod q,\\ M_{S_b} &= \mathcal{H}\big(r_{T_j}\|PID'_{S_b}\big). \end{aligned}$$

S_b aggregates $\{T_1, \ldots, T_J\}$'s messages $\{gid_{T_j}\|V_{T_j}\}$ to establish a backward aggregated-proof AP_b for anonymous data transmission. Here, "Ξ" is defined as the multi-element cascade operation:

$$AP_b = \mathcal{H}(r_{S_b}\|PID'_{S_b}) \oplus \Xi_{j=1}^{J}(gid_{T_j}\|V_{T_j}).$$

S_b further transmits $r_{S_b}\|r_{T_j}\|F_{S_b}\|F_{T_j}\|p_j'^a\|p_b'^a\|M_{S_b}\|AP_b$ to DC_a. Upon receiving the messages, DC_a ascertains $\{S_b, T_j\}$ according to the identity flags $\{F_{S_b}, F_{T_j}\}$, and locally re-computes $\{PID_{T_j}''^{\ell}, PID_{S_b}''^{\ell}\}$:

$$\begin{aligned} PID_{T_j}''^{\ell} &= \mathcal{T}_{l_{DC_a}}\big(p_j'^a\big) \pmod q,\\ PID_{S_b}''^{\ell} &= \mathcal{T}_{l_{DC_a}}\big(p_b'^a\big) \pmod q. \end{aligned}$$

Thereafter, DC_a verifies S_b by re-computing $M_{S_b}^{\ell} = \mathcal{H}(r_{T_j}\|PID_{S_b}''^{\ell})$. Here, $PID_{T_j} \equiv \mathcal{T}_{l_{DC_a}}(\mathcal{F}(p_a^j)) \pmod q$, and $PID_{S_b} \equiv \mathcal{T}_{l_{DC_a}}(\mathcal{F}(p_a^b)) \pmod q$ are applied for verification. If $M_{S_b}^{\ell} = M_{S_b}$ holds, DC_a will regard S_b as a legal sensor; otherwise, the APHA will terminate.

DC_a derives $gid_{T_j}\|V_{T_j}$ by an inverse operation $\Xi^{-1}(.)$, and checks T_j by re-computing $V_{T_j}^{\ell} = \mathcal{H}(r_{T_j}\|PID_{S_b}''^{\ell})$. If $V_{T_j}^{\ell} = V_{T_j}$ holds, DC_a will regard T_j as a legal target; otherwise, the APHA will terminate:

$$gid_{T_j}\|V_{T_j} = \Xi_j^{-1}\big(AP_b \oplus \mathcal{H}\big(r_{S_b}\|PID_{S_b}''^{\ell}\big)\big).$$

3.2.3 Forwards Aggregated-Proof Response and T_j's Verification on S_b

DC_a continues to extract $\{gid_{S_b}, PID_{S_b}, PID_{T_j}, p_{aj}^{jb}\}$ to compute $V_{DC_a}^j$ by the HMAC function:

$$V_{DC_a}^j = \mathcal{H}_{p_{aj}^{jb}}((r_{T_j}\|r_{S_b}) \oplus gid_{S_b}).$$

DC_a establishes a forward aggregated-proof AP_f by wrapping $PID_{T_j}\|V_{DC_a}^j$, and transmits AP_f to S_b:

$$AP_f = \Xi_{j=1}^{J}\big(PID_{T_j}\|V_{DC_a}^j\big) \oplus \mathcal{H}(PID_{S_b}).$$

S_b extracts $\{gid_{S_b}, C_b^j, p_b^j\}$ to obtain the updated values $\{p_b'^j, gid'_{S_b}\}$, computes V_{S_b}, and further transmits $p_b'^j\|V_{S_b}$ to T_j for authentication:

$$\begin{aligned} p_b'^j &= \mathcal{T}_y\big(C_b^j/\mathcal{F}\big(P_b^j\big)\big) \mod q,\\ gid'_{S_b} &= \mathcal{T}_y\big(gid_{S_b}\big) \mod q,\\ V_{S_b} &= AP_f \oplus \mathcal{H}(PID_{S_b}) \oplus \mathcal{H}\big(r_{T_j}\|gid'_{S_b}\big). \end{aligned}$$

T_j computes $|p_{aj}^{jb}|$ and $gid_{S_b}''^{\ell}$ to derive $PID_{T_j}\|V_{DC_a}^j$. Here, $|p_{aj}^{jb}|$ is a mirroring directed path descriptor from DC_a to S_b via T_j:

$$\begin{aligned} |p_{aj}^{jb}| &= \mathcal{F}^{-1}\big(C_j^a/\mathcal{F}\big(p_j^a\big) + \mathcal{F}\big(p_j^b\big)\big),\\ gid_{S_b}''^{\ell} &= \mathcal{T}_{l_{T_j}}\big(p_b'^j\big) \mod q,\\ PID_{T_j}\|V_{DC_a}^j &= \Xi_j^{-1}\big(V_{S_b} \oplus \mathcal{H}\big(r_{T_j}\|gid_{S_b}''^{\ell}\big)\big). \end{aligned}$$

Afterwards, T_j extracts gid_{S_b} to check the validity of S_b by re-computing $V_{DC_a}^{j\ell} = \mathcal{H}_{|p_{aj}^{jb}|\oplus PID_{T_j}}((r_{T_j}\|r_{S_b}) \oplus gid_{S_b})$. If $V_{DC_a}^{j\ell} = V_{DC_a}^j$ holds, T_j will regard S_b as a legal sensor; otherwise, the APHA will terminate.

Till now, S_b and T_j have established the mutual authentication, and DC_a has authenticated $\{T_j, S_b\}$ as legal entities. The backward and forward aggregated-proofs are respectively established to wrap multiple targets $\{T_1, \ldots, T_J\}$'s identity related information.

3.3 The Authentication Protocol in the Ubiquitous IoT

Fig. 3 shows an interaction among $\{DC_a, iDC, nDC\}$, in which DC_a is under iDC's jurisdiction, and $\{DC_a, iDC\}$ are within nDC's management range.

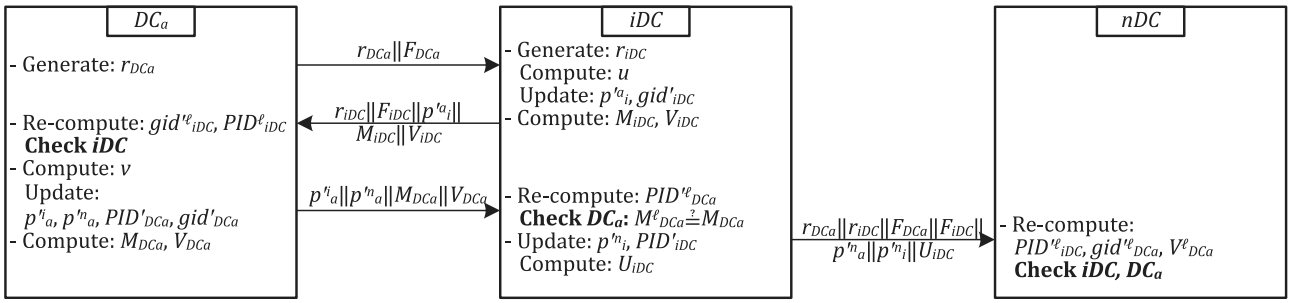

Fig. 3. The authentication protocol in the ubiquitous IoT.

3.3.1 Challenge-Response between DC_a and iDC

DC_a generates a random number r_{DC_a}, extracts its identity flag F_{DC_a}, and transmits $r_{DC_a}\|F_{DC_a}$ to query iDC. Upon receiving the messages, iDC ascertains DC_a's identity by searching the matched F_{DC_a}. Thereafter, iDC generates a random number r_{iDC}, and extracts $\{F_{iDC}, gid_{iDC}, C_i^a, p_i^a\}$. iDC further computes an integer $u = [r_{DC_a}] \pmod e$, and updates $\{p_i^a, gid_{iDC}\}$ into $\{p_i'^a, gid'_{iDC}\}$:

$$p_i'^a = \mathcal{T}_u\big(C_i^a / \mathcal{F}(p_i^a)\big) \pmod q,$$
$$gid'_{iDC} = \mathcal{T}_u(gid_{iDC}) \pmod q.$$

iDC extracts the values $\{gid_{iDC}^n\} = \{gid_{iDC}^1, \ldots, gid_{iDC}^{N_1}\}$, the pseudonyms $\{PID_{DC_a}, PID_{iDC}\}$, and an authentication key k_a to compute $\{M_{iDC}, V_{iDC}\}$. Afterwards, iDC transmits $r_{iDC}\|F_{iDC}\|p_i'^a\|M_{iDC}\|V_{iDC}$ to DC_a for authentication:

$$M_{iDC} = \mathcal{E}_{k_a}(r_{DC_a} \oplus PID_{iDC}),$$
$$V_{iDC} = PID_{DC_a} gid'_{iDC} + \sum_{n=1}^{N_1} \big(gid_{iDC}^n r_{DC_a}\big) \pmod{q^2}.$$

3.3.2 DC_a's Verification on iDC

DC_a extracts $\{\eta_{DC_a}, k_a\}$, locally re-computes $gid_{iDC}'^{\ell}$, and derives PID_{iDC}^{ℓ} by decryption operation:

$$gid_{iDC}'^{\ell} = \mathcal{T}_{l_{DC_a}}\big(p_i'^a\big) \pmod q,$$
$$PID_{iDC}^{\ell} = \mathcal{E}_{k_a}^{-1}(M_{iDC}) \oplus r_{DC_a}.$$

iDC checks DC_a by the following equation according to $gid_{iDC} \equiv \mathcal{T}_{l_{DC_a}}(\mathcal{F}(p_a^i)) \pmod q$ and $PID_{iDC} \equiv \prod_{n=1}^{N_1}(\eta_{DC_a})^{gid_{iDC}^n} \pmod{q^2}$. If it holds, DC_a will regard iDC as a legal industrial data center; otherwise, the APHA will terminate:

$$(\eta_{DC_a})^{V_{iDC}} \stackrel{?}{=} (\eta_{DC_a})^{PID_{DC_a} gid_{iDC}'^{\ell}} (PID_{iDC}^{\ell})^{r_{iDC}} \pmod{q^2}.$$

3.3.3 iDC's Verification on DC_a

DC_a extracts $\{gid_{DC_a}, PID_{DC_a}, C_i^a, C_a^n, p_a^i, p_a^n\}$, and computes an integer $v = [r_{iDC}] \pmod e$. Thereafter, DC_a obtains the updated values $\{p_a'^i, p_a'^n, PID'_{DC_a}, gid'_{DC_a}\}$ for further authentication:

$$p_a'^i = \mathcal{T}_v\big(C_i^a / \mathcal{F}(p_i^a)\big) \pmod q,$$
$$p_a'^n = \mathcal{T}_v\big(C_a^n / \mathcal{F}(p_a^n)\big) \pmod q,$$
$$PID'_{DC_a} = \mathcal{T}_v(PID_{DC_a}) \pmod q,$$
$$gid'_{DC_a} = \mathcal{T}_v(gid_{DC_a}) \pmod q.$$

DC_a extracts gid_{iDC} and $\{gid_{DC_a}^n\}$ to compute $\{M_{DC_a}, V_{DC_a}\}$, and transmits $p_a'^i\|p_a'^n\|M_{DC_a}\|V_{DC_a}$ to iDC:

$$M_{DC_a} = \mathcal{H}\big(r_{iDC}\|PID'_{DC_a}\big),$$
$$V_{DC_a} = gid_{iDC} gid'_{DC_a} + \sum_{n=1}^{N_2} \big(gid_{DC_a}^n r_{DC_a}\big) \pmod{q^2}.$$

iDC locally re-computes $PID_{DC_a}'^{\ell} = \mathcal{T}_{l_{iDC}}(p_a'^i)$ and $M_{DC_a}^{\ell} = \mathcal{H}(r_{iDC}\|PID_{DC_a}'^{\ell})$. According to $PID_{DC_a} \equiv \mathcal{T}_{l_{iDC}}(\mathcal{F}(p_i^a)) \pmod q$, iDC verifies DC_a by comparing whether $M_{DC_a}^{\ell}$ equals M_{DC_a}. If it holds, iDC will regard DC_a as a legal unit data center; otherwise, the APHA will terminate.

3.3.4 nDC's Verification on iDC and DC_a

iDC extracts $\{C_i^n, p_i^n, k_n\}$ to update $\{p_i^n, PID_{iDC}\}$ into $\{p_i'^n, PID'_{iDC}\}$, and computes U_{iDC}. Thereafter, iDC transmits $r_{DC_a}\|r_{iDC}\|F_{DC_a}\|F_{iDC}\|p_a'^n\|p_i'^n\|U_{iDC}$ to nDC for authentication:

$$p_i'^n = \mathcal{T}_u\big(C_i^n / \mathcal{F}\big(p_i^n\big)\big) \pmod q,$$
$$PID'_{iDC} = \mathcal{T}_u(PID_{iDC}) \pmod q,$$
$$U_{iDC} = \mathcal{E}_{k_n}(r_{iDC} \oplus V_{DC_a}) \oplus \mathcal{H}(r_{DC_a}\|PID'_{iDC}).$$

nDC ascertains $\{iDC, DC_a\}$'s identities according to $\{F_{iDC}, F_{DC_a}\}$, and extracts $\{\varphi_{nDC}, gid_{iDC}, PID_{DC_a}, C_n^i, p_n^i, k_n\}$ to re-compute $\{PID_{iDC}'^{\ell}, gid_{DC_a}'^{\ell}, V_{DC_a}^{\ell}\}$:

$$PID_{iDC}'^{\ell} = \mathcal{T}_{l_{nDC}}\big(p_i'^n\big) \pmod q,$$
$$gid_{DC_a}'^{\ell} = \mathcal{T}_{l_{nDC}}\big(p_a'^n\big) \pmod q,$$
$$V_{DC_a}^{\ell} = \mathcal{E}_{k_n}^{-1}\big(U_{iDC} \oplus \mathcal{H}\big(r_{DC_a}\|PID_{iDC}'^{\ell}\big)\big) \oplus r_{iDC}.$$

nDC checks the validity of iDC and DC_a by verifying the following equation according to $PID_{iDC} \equiv \mathcal{T}_{l_{nDC}}(\mathcal{F}(p_n^i))$, $gid_{DC_a} \equiv \mathcal{T}_{l_{nDC}}(\mathcal{F}(p_n^a)) \pmod q$, and $PID_{DC_a} \equiv \prod_{n=1}^{N_2}(\varphi_{nDC})^{gid_{DC_a}^n} \pmod{q^2}$. If it holds, nDC will regard

iDC and DC_a as legal entities; otherwise, the APHA will terminate:

$$(\varphi_{nDC})^{V^{\ell}_{DC_a}} \stackrel{?}{=} (\varphi_{nDC})^{gid_{iDC} gid'^{\ell}_{DC_a}} (PID_{DC_a})^{r_{DC_a}} \pmod{q^2}.$$

Till now, DC_a and iDC have established mutual authentication, and nDC has authenticated $\{DC_a, iDC\}$ as legal entities. Thereinto, iDC and nDC have different access authorities on DC_a's group identifier and pseudonym to achieve hierarchical access control.

3.4 Security Properties

3.4.1 Data Confidentiality and Data Integrity

Data confidentiality is mainly achieved by the Chebyshev chaotic maps, in which the polynomials $\{\mathcal{T}_{l_{T_j}}, \mathcal{T}_{l_{S_b}}, \mathcal{T}_{l_{DC_a}}, \mathcal{T}_{l_{iDC}}, \mathcal{T}_{l_{nDC}}\}$ are defined to represent the relationships of the group identifiers, pseudonyms and directed path descriptors. During the maps, the directed path descriptors are wrapped by the homomorphism function $\mathcal{F}(.)$. Besides, the pseudo-random numbers (i.e., $r_{T_j}, r_{S_b}, r_{DC_a}, r_{iDC}$) are applied to obtain the degree of the Chebyshev polynomials $\{\mathcal{T}_x, \mathcal{T}_y, \mathcal{T}_u, \mathcal{T}_v\}$ for enhancing session randomization.

Data integrity is realized by the one-way hash and HMAC functions. In the unit IoT, $\{M_{T_j}, M_{S_b}, V_{T_j}, V^j_{DC_a}\}$ are transmitted in the terms of $\mathcal{H}(.)$ and $\mathcal{H}_{p^{jb}_{aj}}(.)$ for identify declaration and verification. In the ubiquitous IoT, $\{M_{DC_a}, U_{iDC}\}$ are respectively challenged to wrap PID'_{DC_a} and PID'_{iDC} into hash functions for verifying DC_a and iDC. Note that the one-way values apply pseudo-random numbers, which can ensure that attackers cannot derive the private values for data corruption.

3.4.2 Hierarchical Access Control

Two-layered interactions of $\{T_j, S_b, DC_a\}$ and $\{DC_a, iDC, nDC\}$ are performed in relatively independent modes, during which DC_a acts as a media to connect the unit IoT and ubiquitous IoT. According to the practical application requirements, $\{T_j, S_b, DC_a, iDC, nDC\}$ are assigned the different access authorities in the U2IoT.

- For T_j. T_j owns S_b's group identifier gid_{S_b} to ascertain the general group attribute, and ensure that only an in-group sensor can access T_j's data.
- For S_b. S_b can only determine T_j's group identifier gid_{T_j} by the challenged pseudo-random identity flag F_{T_j} without obtaining the pseudonym PID_{T_j} to restrain S_b's access authority on T_j.
- For DC_a. In the unit IoT, DC_a owns reinforced access authorities on $\{T_j, S_b\}$, and can ascertain $\{T_j, S_b\}$'s detailed group identifiers $\{gid_{T_j}, gid_{S_b}\}$ based on the flags. Additionally, DC_a can further determine $\{T_j, S_b\}$'s pseudonyms $\{PID_{T_j}, PID_{S_b}\}$ for further management. In the ubiquitous IoT, DC_a owns iDC's group identifier gid_{iDC} to ensure that only the industrial data center with the appointed group identifier can access DC_a's data.
- For iDC. iDC owns DC_a's pseudonym PID_{DC_a} to realize that iDC can ascertain DC_a's detailed identity in an industry application.
- For nDC. nDC owns access authorities on both unit IoT and industrial IoT. DC_a's pseudonym PID_{DC_a} and iDC's group identifier gid_{iDC} are available to realize the centralized management.

3.4.3 Forward Unlinkability

The pseudo-random numbers are generated as session-sensitive operators to provide session freshness and randomization. Additionally, the identity related values (e.g., identify flags, group identifier, and pseudonym) are dynamically updated during each session. Such variables are applied to obtain the authentication operators (e.g., $V_{T_j}, M_{S_b}, M_{DC_a}$, and V_{iDC}), the aggregated-proofs, and other intermediate variables (e.g., V_{S_b}). The transmitted messages are mainly computed based on the random numbers $\{r_{T_j}, r_{S_b}, r_{DC_a}, r_{iDC}\}$, which make that the exchanged messages can be regarded as dynamically variables with perfect forward unlinkability, and an attacker cannot correlate the ongoing session with former sessions in the open channels.

3.4.4 Mutual Authentication

In the unit IoT, the mutual authentication is established between T_j and S_b, and authentication operators are applied to check the identity correctness and consistency. The Chebyshev chaotic maps $gid_{T_j} \equiv \mathcal{T}_{l_{S_b}}(\mathcal{F}(p^j_b)) \pmod{q}$ and $gid_{S_b} \equiv \mathcal{T}_{l_{T_j}}(\mathcal{F}(p^b_j)) \pmod{q}$ are used for authentication; The pairwise directed path descriptors $\{p^j_b, p^b_j\}$ can be derived by $\mathcal{F}(p^b_j p^j_b) = \mathcal{F}(p^b_j)\mathcal{F}(p^j_b) = C^j_b = C^b_j$; The mirroring directed path descriptor $|p^{jb}_{aj}|$ is obtained by $\mathcal{F}(|p^{jb}_{aj}|) = \mathcal{F}(p^b_j + p^j_a) = \mathcal{F}(p^b_j) + \mathcal{F}(p^j_a)$.

In the ubiquitous IoT, hybrid authentications are established among $\{DC_a, iDC, nDC\}$. The Chebyshev chaotic maps $\{\mathcal{T}_{l_{DC_a}}, \mathcal{T}_{l_{iDC}}, \mathcal{T}_{l_{nDC}}\}$ are introduced for authentication. Besides, the group identifiers $\{gid_{iDC}, gid_{DC_a}\}$ can be extended into $\{gid^1_{iDC}, \ldots, gid^{N_1}_{iDC}\}$ and $\{gid^1_{DC_a}, \ldots, gid^{N_2}_{DC_a}\}$, which satisfy the pre-shared relationships with the corresponding pseudonyms $\{PID_{iDC}, PID_{DC_a}\}$.

3.4.5 Privacy Preservation

The backward aggregated-proof AP_b is established by S_b to wrap multiple targets $\{T_1, \ldots, T_J\}$'s identity related values, and the cascaded value $\Xi^J_{j=1}(gid_{T_j} \| V_{T_j})$ is further XORed by the hash value $\mathcal{H}(r_{S_b} \| PID'_{S_b})$ for anonymous data transmission. Here, AP_b covers the wrapped values $\mathcal{T}_x(PID_{T_j})$ and $\mathcal{T}_y(PID_{S_b})$. Here, the multi-element cascade operators $\Xi^J_{j=1}(.)$ and its inverse operation Ξ^{-1}_j are defined for aggregation and derivation. The forward aggregated-proof AP_f is established by DC_a to respond $\{T_1, \ldots, T_J\}$. Note that AP_f includes the cascaded value $(PID_{T_1} \| V^1_{DC_a}) \| , \ldots, \| \ (PID_{T_J} \| V^J_{DC_a})$, and $\{T_j\}$ can respectively derive $\{PID_{T_j} \| \ V^j_{DC_a}\}$ to authenticate S_b.

The aggregated-proofs have two main functions: one is to pack multiple targets' challenges into a group, and the other

TABLE 3
The Formal Notations

Notation	Description
$P \mid\equiv X$	P believes X, or P would be entitled to believe X.
$P \lhd X$	P receives X, and can repeat X.
$P \mid\sim X$	P conveyed X, and believes X.
$P \mid\Rightarrow X$	P has jurisdiction on X.
$\sharp(X)$	X is fresh, and has never been sent before.
$P \overset{K}{\leftrightarrow} Q$	K is a good key shared by P and Q.
$\overset{K}{\mapsto} P$	P has a public key K.
$P \overset{X}{\Leftrightarrow} Q$	X is a secret known to P and Q.
$\{X\}_K$	X is encrypted with the key K.
$\langle X \rangle_Y$	i.e., $\langle X, Y \rangle$, X is combined with a secret Y.

is to pack DC_a's responses into a group. Such aggregated data transmission realizes that $\{T_j\}$'s individual identity related information cannot be revealed, and attackers cannot derive individual sensitive information according to the intercepted messages. It turns out that only the legal unit data center can derive each target's identity information by AP_b, and only the legal target can derive its authorized fields by AP_f.

4 Formal Analysis with the BAN Logic

In this section, Burrows-Abadi-Needham (i.e., BAN) logic [26] is applied to analyze the design correctness for security proof, and it is a rigorous evaluation method to detect subtle defects for authentication scheme. The formal analysis focuses on belief and freshness, involving the following steps: message formalization, initial assumptions declaration, anticipant goals declaration, and logic verification. Table 3 shows formal notations in the BAN logic.

4.1 Message Formalization

Message formalization is to specify the exchanged messages. In the unit IoT, the formalized messages among $\{DC_a, S_b, T_j\}$ are obtained as follows:

M1.1: $T_j \lhd r_{S_b}, T_j \lhd F_{S_b}$;
M1.2: $S_b \lhd r_{T_j}, S_b \lhd F_{T_j}$,
$S_b \lhd \langle r_{S_b}, p_j^a \rangle_{C_j^a}, S_b \lhd \langle r_{S_b}, p_j^b \rangle_{C_j^b}$,
$S_b \lhd M_{T_j}, S_b \lhd V_{T_j}$;
M1.3: $DC_a \lhd r_{S_b}, DC_a \lhd r_{T_j}$,
$DC_a \lhd F_{S_b}, DC_a \lhd F_{T_j}$,
$DC_a \lhd \langle r_{S_b}, p_j^a \rangle_{C_a^a}, DC_a \lhd \langle r_{T_j}, p_b^a \rangle_{C_b^a}$,
$DC_a \lhd M_{S_b}, DC_a^j \lhd AP_b$;
M1.4: $S_b \lhd AP_f$;
M1.5: $T_j \lhd \langle r_{T_j}, p_b^j \rangle_{C_b^j}, T_j \lhd V_{S_b}$.

In the ubiquitous IoT, the formalized messages among $\{DC_a, iDC, nDC\}$ are obtained as follows:

M2.1: $iDC \lhd r_{DC_a}, iDC \lhd F_{DC_a}$;
M2.2: $DC_a \lhd r_{iDC}, DC_a \lhd F_{iDC}, DC_a \lhd \langle r_{DC_a}, p_i^a \rangle_{C_i^a}$,
$DC_a \lhd \{r_{DC_a}, PID_{iDC}\}_{k_a}, DC_a \lhd V_{iDC}$;
M2.3: $iDC \lhd \langle r_{iDC}, p_a^i \rangle_{C_a^i}, iDC \lhd \langle r_{iDC}, p_a^n \rangle_{C_a^n}$,
$iDC \lhd M_{DC_a}, iDC \lhd V_{DC_a}$;
M2.4: $nDC \lhd r_{DC_a}, nDC \lhd r_{iDC}$,
$nDC \lhd F_{DC_a}, nDC \lhd F_{iDC}$,
$iDC \lhd \langle r_{iDC}, p_a^n \rangle_{C_a^n}, iDC \lhd \langle r_{DC_a}, p_i^n \rangle_{C_i^n}$,
$nDC \lhd U_{iDC}$.

4.2 Initial Assumptions

In the APHA, an entity believes that: 1) the shared secrets and keys are obtained by the assigned entities, 2) the pseudo random numbers, identity flags, pseudonyms, and directed path descriptors are fresh, and 3) the trusted entity has jurisdiction on the entitled values. The initiative assumptions, including initial possessions and entity abilities are obtained as follows:

- For T_j:
  P1.1: $T_j \mid\equiv S_b \overset{F_{T_j}, F_{S_b}, gid_{T_j}, gid_{S_b}, C_j^b}{\Longleftrightarrow} T_j$,
  $T_j \mid\equiv DC_a \overset{F_{T_j}, gid_{T_j}, PID_{T_j}, C_j^a}{\Longleftrightarrow} T_j$;
  P1.2: $T_j \mid\equiv \sharp(r_{T_j}, F_{T_j}, PID_{T_j}, p_j^a, p_j^b)$;
  P1.3: $T_j \mid\equiv (DC_a \mid\Rightarrow (F_{T_j}, gid_{T_j}, PID_{T_j}, p_{aj}^{jb}))$.
- For S_b:
  P2.1: $S_b \mid\equiv T_j \overset{F_{T_j}, F_{S_b}, gid_{T_j}, gid_{S_b}, C_b^j}{\Longleftrightarrow} S_b$,
  $S_b \mid\equiv DC_a \overset{F_{S_b}, gid_{S_b}, PID_{S_b}, C_b^a}{\Longleftrightarrow} S_b$;
  P2.2: $S_b \mid\equiv \sharp(r_{S_b}, F_{S_b}, PID_{S_b}, p_b^a)$;
  P2.3: $S_b \mid\equiv (DC_a \mid\Rightarrow (F_{S_b}, gid_{S_b}, PID_{S_b}))$.
- For DC_a:
  P3.1: $DC_a \mid\equiv T_j \overset{F_{T_j}, gid_{T_j}, PID_{T_j}, C_a^j}{\Longleftrightarrow} DC_a$,
  $DC_a \mid\equiv S_b \overset{F_{S_b}, gid_{S_b}, PID_{S_b}, C_a^b}{\Longleftrightarrow} DC_a$,
  $DC_a \mid\equiv iDC \overset{F_{DC_a}, F_{iDC}, gid_{iDC}, PID_{DC_a}, C_a^i}{\Longleftrightarrow} DC_a$,
  $DC_a \mid\equiv nDC \overset{F_{DC_a}, PID_{DC_a}}{\Longleftrightarrow} DC_a$;
  P3.2: $DC_a \mid\equiv iDC \overset{k_a}{\longleftrightarrow} DC_a$,
  P3.3: $DC_a \mid\equiv \sharp(r_{DC_a}, F_{DC_a}, gid_{DC_a}, PID_{DC_a})$,
  $DC_a \mid\equiv \sharp(p_{aj}^{jb}, p_a^i, p_a^n)$;
  P3.4: $DC_a \mid\equiv (nDC \mid\Rightarrow (F_{DC_a}, PID_{DC_a}))$.
- For iDC:
  P4.1: $iDC \mid\equiv DC_a \overset{F_{DC_a}, F_{iDC}, gid_{iDC}, PID_{DC_a}, C_i^a}{\Longleftrightarrow} iDC$,
  $iDC \mid\equiv nDC \overset{F_{iDC}, gid_{iDC}, C_i^n}{\Longleftrightarrow} iDC$;
  P4.2: $iDC \mid\equiv DC_a \overset{k_a}{\longleftrightarrow} iDC$,
  $iDC \mid\equiv nDC \overset{k_n}{\longleftrightarrow} iDC$;
  P4.3: $iDC \mid\equiv \sharp(r_{iDC}, F_{iDC}, gid_{iDC}, PID_{iDC}, p_i^a, p_i^n)$;
  P4.4: $iDC \mid\equiv (nDC \mid\Rightarrow (F_{iDC}, gid_{iDC}))$.
- For nDC:
  P5.1: $nDC \mid\equiv DC_a \overset{F_{DC_a}, PID_{DC_a}}{\Longleftrightarrow} nDC$,
  $nDC \mid\equiv iDC \overset{F_{iDC}, gid_{iDC}, C_n^i}{\Longleftrightarrow} nDC$;
  P5.2: $nDC \mid\equiv iDC \overset{k_n}{\longleftrightarrow} nDC$;
  P5.3: $nDC \mid\equiv \sharp(p_n^i)$;

4.3 Anticipant Goals

The security goals refer to belief and freshness, in which the exchanged messages are transmitted from authenticated entities, and the messages were never used in former sessions. In the APHA, the anticipant goals are obtained as follows:

- In the unit IoT:
  G1.1: $T_j \mid\equiv S_b \mid\sim p_b^j$,
  G1.2: $T_j \mid\equiv \sharp V_{S_b}$,

G1.3: $S_b \mid \equiv T_j \mid \sim p_j^b$,
G1.4: $S_b \mid \equiv \sharp(p_j'^a, p_j'^b, M_{T_j}, AP_f)$,
G1.5: $S_b \mid \equiv DC_a \overset{gid_{T_j}, PID_{T_j}}{\Longleftrightarrow} T_j$,
G1.6: $DC_a \mid \equiv T_j \mid \sim p_j^a$,
G1.7: $DC_a \mid \equiv S_b \mid \sim p_b^a$.

- In the ubiquitous IoT:
  G2.1: $DC_a \mid \equiv iDC \mid \sim (p_i^a, PID_{iDC})$,
  G2.2: $DC_a \mid \equiv \sharp(p_i'^a, M_{iDC})$,
  G2.3: $iDC \mid \equiv DC_a \mid \sim p_a^i$,
  G2.4: $iDC \mid \equiv \sharp(p_a'^i, p_a'^n, M_{DC_a})$,
  G2.5: $iDC \mid \equiv nDC \overset{PID_{DC_a}}{\Longleftrightarrow} DC_a$,
  G2.6: $nDC \mid \equiv DC_a \mid \sim p_a^n$,
  G2.7: $nDC \mid \equiv iDC \mid \sim (p_i^n, V_{DC_a})$.

4.4 Logic Verification

Logic verification is performed according to the formalized messages, initial assumptions, and the related rules of the BAN logic.

Theorem 1.1. *T_j believes that S_b conveyed p_j^b.*

Proof: According to P1.1: $T_j \mid \equiv S_b \overset{C_j^b}{\Longleftrightarrow} T_j$, it turns out that T_j believes that C_j^b is a shared secret with S_b.

According to M1.5: $T_j \lhd \langle r_{T_j}, p_b^j \rangle_{C_b^j}$, it turns out that T_j receives $\langle r_{T_j}, p_b^j \rangle_{C_b^j}$. Due to $C_b^j = C_j^b$, we obtain that $T_j \lhd \langle r_{T_j}, p_b^j \rangle_{C_j^b}$. Applying the message-meaning rule (RM3):

$$\frac{P \mid \equiv Q \overset{Y}{\Longleftrightarrow} P, P \lhd \langle X \rangle_Y}{P \mid \equiv Q \mid \sim X},$$

we obtain that,

$$T_j \mid \equiv S_b \mid \sim (r_{T_j}, p_b^j).$$

If T_j believes that C_j^b is a shared secret with S_b, and T_j receives $\langle r_{T_j}, p_b^j \rangle_{C_b^j}$, T_j will believe that S_b once conveyed the message (r_{T_j}, p_b^j). Thereafter, applying the belief rule (RB4): $\frac{P \mid \equiv Q \mid \sim (X,Y)}{P \mid \equiv Q \mid \sim X}$, we obtain that,

$$T_j \mid \equiv S_b \mid \sim p_b^j.$$

If T_j believes that S_b conveyed the message (r_{T_j}, p_b^j), T_j will believe that S_b conveyed the sub-message p_b^j. Note that the postulate is sound because the rules for $\lhd$ guarantee that p_b^j was not just uttered by T_j. Till now, G1.1 has been proven, and G1.3, G1.6, G1.7, G2.3, and G2.6 can be achieved via the similar procedures. □

Theorem 1.2. *DC_a believes that iDC conveyed p_i^a and PID_{iDC}.*

Proof. Similarly, according to $DC_a \mid \equiv iDC \overset{C_a^i}{\Longleftrightarrow} DC_a, DC_a \lhd \langle r_{DC_a}, p_i^a \rangle_{C_i^a}$, RM3, and RB4, we obtain that $DC_a \mid \equiv iDC \mid \sim p_i^a$.

According to P3.2: $DC_a \mid \equiv iDC \overset{k_a}{\longleftrightarrow} DC_a$, it turns out that DC_a believes that k_a is a good key shared by iDC and DC_a.

According to M2.2: $DC_a \lhd \{r_{DC_a}, PID_{iDC}\}_{k_a}$, it turns out that DC_a receives $\{r_{DC_a}, PID_{iDC}\}_{k_a}$, in which a secret key k_a is applied for establishing the ciphertext. Applying the message-meaning rule (RM1): $\frac{P \mid \equiv Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\}_K}{P \mid \equiv Q \mid \sim X}$, we obtain that,

$$DC_a \mid \equiv iDC \mid \sim (r_{DC_a}, PID_{iDC}).$$

If DC_a believes that k_a is a shared key with iDC, and DC_a receives the wrapped message $\{r_{DC_a}, PID_{iDC}\}_{k_a}$, DC_a will believe that S_b conveyed (r_{DC_a}, PID_{iDC}). Applying the belief rule (RB4): $\frac{P \mid \equiv Q \mid \sim (X,Y)}{P \mid \equiv Q \mid \sim X}$, we obtain that,

$$DC_a \mid \equiv iDC \mid \sim PID_{iDC}.$$

If DC_a believes that S_b once conveyed the message (r_{DC_a}, PID_{iDC}), DC_a will believe that S_b conveyed the sub-message PID_{iDC}. Till now, G2.1 has been proven, and G2.7 can be achieved via the similar procedures. □

Theorem 2. *T_j believes that V_{S_b} is fresh.*

Proof. According to P1.2: $T_j \mid \equiv \sharp(r_{T_j}, PID_{T_j})$, it turns out that T_j believes that $\{r_{T_j}, PID_{T_j}\}$ are fresh.

According to M1.5: $T_j \lhd V_{S_b}$, in which V_{S_b} contains the elements $\{p_{aj}^{jb}, r_{T_j}, r_{S_b}, gid_{S_b}, PID_{T_j}, PID_{S_b}\}$, and it is randomized by $\{r_{T_j}, PID_{T_j}\}$. Applying the freshness rule (RF1): $\frac{P \mid \equiv \sharp(X)}{P \mid \equiv \sharp(X,Y)}$, we obtain that,

$$T_j \mid \equiv \sharp V_{S_b}.$$

If T_j believes that $\{r_{T_j}, PID_{T_j}\}$ are fresh, T_j will also believe that V_{S_b} is fresh. Till now, G1.2 has been proven, and G1.4, G2.2, and G2.4 can be achieved via the similar procedures. □

Theorem 3. *S_b believes that gid_{T_j} and PID_{T_j} are secrets shared by $\{DC_a, T_j\}$.*

Proof. According to the secure communication channel between S_b and DC_a, we obtain that,

$$S_b \mid \equiv DC_a \mid \Rightarrow (DC_a \mid \equiv *),$$
$$S_b \mid \equiv DC_a \mid \equiv (DC_a \mid \equiv *).$$

According to P3.1: $DC_a \mid \equiv T_j \overset{gid_{T_j}, PID_{T_j}}{\Longleftrightarrow} DC_a$, it turns out that DC_a believes that $\{gid_{T_j}, PID_{T_j}\}$ are shared by $\{DC_a, T_j\}$. Applying the secret sharing rule (RK3):

$$\frac{P \mid \equiv R \overset{X}{\Longleftrightarrow} R'}{P \mid \equiv R' \overset{X}{\Longleftrightarrow} R}.$$

We obtain that $DC_a \mid \equiv DC_a \overset{gid_{T_j}, PID_{T_j}}{\Longleftrightarrow} T_j$. According to $S_b \mid \equiv DC_a \mid \Rightarrow (DC_a \mid \equiv *)$ and $S_b \mid \equiv DC_a \mid \equiv (DC_a \mid \equiv *)$, we obtain that,

$$S_b| \equiv DC_a| \Rightarrow \left(DC_a \overset{gid_{T_j}, PID_{T_j}}{\Longleftrightarrow} T_j\right),$$

$$S_b| \equiv DC_a| \equiv \left(DC_a \overset{gid_{T_j}, PID_{T_j}}{\Longleftrightarrow} T_j\right).$$

Thereafter, applying the jurisdiction rule (RJ1): $\frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$, we obtain that,

$$S_b| \equiv DC_a \overset{gid_{T_j}, PID_{T_j}}{\Longleftrightarrow} T_j.$$

If S_b believes that DC_a is trusted, S_b believes that DC_a believes that the secrets $\{gid_{T_j}, PID_{T_j}\}$ are shared by $\{DC_a, T_j\}$, and S_b believes that DC_a has jurisdiction over $_{DC_a} \overset{F_{MC_{aj}}}{\Longleftrightarrow} T_j, S_b$ will trust DC_a on the truth of $_{DC_a} \overset{F_{MC_{aj}}}{\Longleftrightarrow} T_j$. Till now, G1.5 has been proven, and G2.5 can be achieved via the similar procedures.

Thus, the BAN logic based security proof is demonstrated for formal analysis. In APHA, $\{T_j, S_b\}$ and $\{DC_a, iDC\}$ can respectively establish beliefs via the mutual authentication, and the APHA is proved to be correct and ensures nonexistence of obvious design defects. □

5 Conclusion

In this paper, we have proposed an aggregated-proof based hierarchical authentication scheme for the U2IoT architecture. In the APHA, two sub-protocols are respectively designed for the unit IoT and ubiquitous IoT to provide bottom-up security protection. The proposed scheme realizes data confidentiality and data integrity by the directed path descriptor and homomorphism based Chebyshev chaotic maps, establishes trust relationships via the lightweight mechanisms, and applies dynamically hashed values to achieve session freshness. It indicates that the APHA is suitable for the U2IoT architecture.

Acknowledgments

This work was funded by DNSLAB, China Internet Network Information Center, Beijing 100190, China.

References

[1] B. Guo, D. Zhang, Z. Yu, Y. Liang, Z. Wang, and X. Zhou, "From the internet of things to embedded intelligence," *World Wide Web J.*, vol. 16, no. 4, pp. 399–420, 2013.
[2] R. H. Weber, "Internet of things—New security and privacy challenges," *Comput. Law Security Rev.*, vol. 26, no. 1, pp. 23–30, 2010.
[3] H. Ning and Z. Wang, "Future internet of things architecture: Like mankind neural system or social organization framework?" *IEEE Commun. Lett.*, vol. 15, no. 4, pp. 461–463, Apr. 2011.
[4] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Comput.*, vol. 44, no. 9, pp. 51–58, 2011.
[5] K. Lampropoulos and S. Denazis, "Identity management directions in future internet," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 74–83, Dec. 2011.
[6] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based internet of things," *Wireless Pers. Commun.*, vol. 61, no. 3, pp. 527–542, 2011.
[7] F. V. Meca, J. H. Ziegeldorf, P. M. Sanchez, O. G. Morchon, S. S. Kumar, and S. L. Keoh, "HIP security architecture for the IP-based internet of things," in *Proc. 27th Int. Conf. Adv. Inform. Netw. Appl. Workshops*, 2013, pp. 1331–1336.
[8] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," *Comput.*, vol. 46, no. 4, pp. 46–53, 2013.
[9] G. P. Hancke, K. Markantonakis, and K. E. Mayes, "Security challenges for user-oriented RFID applications within the "internet of things"," *J. Internet Technol.*, vol. 11, no. 3, pp. 307–313, 2010.
[10] T. Yan and Q. Wen, "Building the internet of things using a mobile RFID security protocol based on information technology," *Adv. Intell. Soft Comput.*, vol. 104, pp. 143–149, 2011.
[11] K. Toumi, M. Ayari, L. A. Saidane, M. Bouet, and G. Pujolle, "HAT: HIP address translation protocol for hybrid RFID/IP internet of things communication," in *Proc. Int. Conf. Commun. Wireless Environ. Ubiquitous Syst.: New Challenges*, 2010, pp. 1–7.
[12] K. Chang and J. Chen, "A survey of trust management in WSNs, internet of things and future internet," *KSII Trans. Internet Inform. Syst.*, vol. 6, no. 1, pp. 5–23, 2012.
[13] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the internet of things," *IEEE Sens. J.*, vol. 13, no. 10, pp. 3711–3720, Oct. 2013.
[14] X. Yao, X. Han, X. Du, and X. Zhou, "A lightweight multicast authentication mechanism for small scale IoT applications," *IEEE Sens. J.*, vol. 13, no. 10, pp. 3693–3701, Oct. 2013.
[15] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Comput. Elect. Eng.*, vol. 37, no. 2, pp. 147–159, 2011.
[16] F. Ren and J. Ma, "Attribute-based access control mechanism for perceptive layer of the internet of things," *Int. J. Digital Content Technol. Appl.*, vol. 5, no. 10, pp. 396–403, 2011.
[17] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," *Comput. Sci. Inform. Syst.*, vol. 8, no. 4, pp. 1207–1228, 2011.
[18] X. Wang, X. Sun, H. Yang, and S. A. Shah, "An anonymity and authentication mechanism for internet of things," *J. Convergence Inform. Technol.*, vol. 6, no. 3, pp. 98–105, 2011.
[19] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for internet of things," in *Proc. Int. Conf. Model., Identification Control*, 2011, pp. 563–566.
[20] L. Zhou and H. C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Netw.*, vol. 25, no. 3, pp. 35–40, May/Jun. 2011.
[21] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: An internet of things application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, Nov. 2011.
[22] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.
[23] T. Zhang, Q. Wu, W. Liu, and L. Chen, "Homomorphism encryption algorithm for elementary operations over real number domain," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov.*, pp. 166–169, 2012.
[24] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*. Boca Raton, FL, USA: CRC Press, 2003.
[25] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons Fractals*, vol. 37, no. 3, pp. 669–674, 2008.
[26] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

Huansheng Ning received the BS degree from Anhui University and the PhD degree from Beihang University, in 1996 and 2001, respectively. He is a professor in the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. His current research interests include internet of things, aviation security, electromagnetic sensing, and computing. He has published more than 50 papers in journals, international conferences/workshops. He is a senior member of the IEEE.

Hong Liu is currently working toward the PhD degree from the School of Electronic and Information Engineering, Beihang University, China. She focuses on the security and privacy issues in radio frequency identification, vehicle-to-grid (V2G) networks, and internet of things. Her research interests include authentication protocol design, and security formal modeling and analysis. She is a student member of the IEEE.

Laurence T. Yang received the BE degree in computer science from Tsinghua University, China, and the PhD degree in computer science from the University of Victoria, Canada. He is a professor in the School of Computer Science and Technology at the Huazhong University of Science and Technology, China, and in the Department of Computer Science, St. Francis Xavier University, Canada. His research interests include parallel and distributed computing, and embedded and ubiquitous/pervasive computing. His research is supported by the National Sciences and Engineering Research Council and the Canada Foundation for Innovation. He is a member of the IEEE.