An Authentication Framework in ICN-Enabled Industrial Cyber-Physical Systems

Yanrong Lu[1,2(✉)], Mengshi Zhang[3], and Xi Zheng[4]

[1] School of Computer Science and Technology, Civil Aviation University of China, Tianjin, China
luyanrong1985@163.com
[2] Tianjin Key Laboratory of Intelligence Computing and Novel Software Technology, Tianjin University of Technology, Tianjin, China
[3] Facebook Inc., Menlo Park, CA, USA
[4] Autonomous Systems Research Center Australia, Brisbane, Australia

Abstract. Industrial Cyber-Physical Systems (ICPS), as a new industrial revolution, are to provide advanced intellectual foundation for next generation industrial systems. While such systems present substantial security challenges for the host-centric communication with the growing trend of sensor data streams. Information Centric Networking (ICN) architecture suggests features exploitable in ICPS applications, reducing delivery latency and promoting quality of services that applies broadly across Industrial Internet. Emerging available solutions for secure communication, however, few of them have thoroughly addressed concerns related to securing access due to the dependence on an online provider server. In this work, we propose a concrete authentication framework for ICN ICPS based on proxy signature, which guarantees authentic sensor data access only to legitimate users and does not require interaction between users. This framework would help lower the level of the complexity of the entire system and reduce the cost of authentication by leveraging edge cache. We prove the security of the proposed authentication scheme and present performance analysis to show its efficiency.

Keywords: Information Centric Networking (ICN) · Industrial Cyber-Physical System (ICPS) · Authentication

1 Introduction

The emergence Industrial 4.0 enables existing factory world to be more flexible, efficient and smart. Currently, wireless technology speeds up the deployment of Industrial 4.0 at a reasonable economic cost and with reduced energy

Supported in part by the National Natural Science Foundation of China under Grants 61802276 and in part by the Opening Foundation of Tianjin Key Laboratory of Intelligence Computing and Novel Software Technology, Tianjin University of Technology, China.

D. Wang et al. (Eds.): SPNCE 2020, LNICST 344, pp. 223–243, 2021.
https://doi.org/10.1007/978-3-030-66922-5_15

and resources consumption [17]. With such direction, industries have shifted their concern to intelligent realizing and controlling processes with an acceptable quality of experience for their users. Based on these benefits, Industrial Cyber-Physical Systems (ICPS) as a new paradigm provides a variety of advantages for cooperative communication to significantly improve service quality and reduce expenditure for the infrastructure. Despite its many attractive features including adaptability, reliability, data integration, automation and optimization, ICPS is faced with high complexity, inefficient distribution control as well as security and privacy issues [2,3].

Moreover, according to Cisco's global mobile data traffic forecast, by 2021 [1], the amount of device will generate 77 billion tb of traffic per month. ICPS communication networks will be an important part of communication between devices. This implies that huge amount of data generated by device and advanced sensor technology deployed in ICPS, which has posed significant challenges on the current host centric-based communication model. The quest for the ever-increasing demand of bandwidth has not been addressed adequately by the existing Internet infrastructure. On the other hand, such tremendous data delivery leads to complicate network management and ICPS application development (e.g. smart grid, smart manufacturing, smart health), which mismatches quality of user experience. Along these lines, one of the most challenging tasks is to offer reliable communication from the source towards destination enabling real-time monitor of supply and demand balances with lower latency.

To cope with these forementioned challenges, a scalable networking architecture that satisfies ICPS communication requirements is imperative. Information Centric Networking (ICN), as one of promising approaches, shifts the current Internet infrastructure from a host-centric paradigm to content-based model in which information source is separated from where information is needed. This decoupling of information from the exact location enables a higher degree of flexibility, especially in supporting device-to-device content sharing [5,6]. Thus, ICN is considered as one of an ideal underlying communication stack for ICPS since it has a great advantage in eliminating transmission latency.

Taking smart grid, a typical ICPS applications, as an example. There could be a power server which is in charge of monitoring, managing, and coordinating the energy consumption, and allows its subscribed users to benefit from real-time electricity consumption data. With the integration of ICN into ICPS, a terminal user only needs to express its interest with content name from multiple devices, to the specific sensor or actuator that provides the information instead of the hosts. Since a copy of the data is cached in along router once an energy data is fetched from the power server, thus allowing further requests with the same name to be fulfilled quickly.

Yet, in spite of those advantages, the deployment of ICN on ICPS poses some new challenges, among which authentication is a high-ranking one. In the IP-based solution, before a user retrieves some sensor data from devices, the session connection is provided such that end-to-end trust is easily established [4, 10,12,18]. However, due to the in-network cache in ICN, the unpredictability

with which repositories provide data leads to difficulty in preventing fake data injection attacks. Similarly, any requests can be satisfied by the routers results in attackers pretend to be a trusted individual to gain access and manipulate the system. To combat these threats, users and routers need to verify data before retrieving or caching them while the identities of users also need to be verified. Therefore, a concrete and efficient authentication instantiation is needed for the implement of ICN in ICPS model.

In this paper, we present an authentication scheme under ICN-enabled architecture to provide user-to-user communication service for ICPS. We describe an ICPS framework that addresses authentication of users and supports user-to-user authentication based on ICN paradigm. To authenticate and save computational consumption on ICPS devices, proxy signature as a building block is enforced so that content integrity is preserved. To separate authentication from ICPS devices, we leverage the edge router close to the users, to authenticate the users' requests. It is believed that by taking advantage of these operations, content transmission can be more robust, with lower latency and less complexity as compared with existing work. To summarize, we make four-fold contributions:

- We provide a two-layer security framework for ICN-based ICPS. The upper layer provides registration service, while the lower layer employs sensor data transmission. It obviates the need for a direct connection with ICPS devices and lower the level of complexity of the system;
- We develop a proxy signature that enables computational savings of ICPS devices. It preserves the privacy privileges of original signer and proves unforgeable in the random oracle;
- We propose a session-based scheme that relies on the proxy signature to ensure user authentication. It ensures that authentic sensor data are only available by legitimate users;
- We present security and performance of the proposed approach to show its robustness and effectiveness compared to existing work.

The roadmap of this article is organized as follows. We state our system model, threat model, and objectives in Sect. 2. We then present our proxy signature in Sect. 3 and the construction of our whole scheme in Sect. 4. Security analysis is shown in Sect. 5 and performance analysis is presented in Sect. 6. Finally, we make a conclusion in Sect. 7.

1.1 Related Work

Current solutions for access security in ICN framework are content authenticity in the sense that a user signs on the requested content, such as [21] or content confidentiality in the sense that a user encrypts the requested content, such as [9,13]. Content authenticity, for example, Zheng *et al.* [21] proposed a certificateless-based signature with revocation to prevent false data injection. The scheme realizes provider authentication so that any receiver could identify the source of the data. Moreover, it largely decreases content verification

overhead compared to public key signature algorithms. Current content confidentiality, for example, Fotiou *et al.* [9] suggested an identity-based cryptography (IBC) based proxy re-encryption scheme. Since there is no need to manage (e.g., issue and revoke) public-key certificates in IBC schemes, this scheme significantly reduces the computational overhead compared to public key infrastructure-based schemes. Still, it needs to pre-store encryption keys and thus is impractical for large-scale deployments. Li *et al.* [13] presented an attribute-based encryption for access control enforcement in ICN, and the symmetric key used to encrypt the data generated by attributes of an authorized user. Despite its low overhead, revocation remains a challenge in such approach, for the private keys corresponding to each attribute have to be regenerated and redistributed during revocation. Other schemes that are considered under proxy broadcast encryption [15] and re-encryption [7], indeed these schemes contribute for computational cost, but has vulnerabilities such as denial-of-service attack scenario.

Coming up with different solutions, many researchers have contributed to the hybrid approaches. Xue *et al.* [19] designed a mechanism built upon group signature and symmetric cryptographic operations, where all of keys are generated by a trusted provider. With such design, user privacy and data confidentiality are both achieved. However, each user needs to get the necessary secret information through a secure channel from the provider, which requires the provider and users to be directly connected thus offsetting the benefits of in-network caching. Nunes-Tsudik [16] proposed a scheme in which the authentication request is sent to the network through Kerberos enforcement aiming to reduce the vulnerability of the user. A hybrid authentication and authorization based on trusted platform that could provide considerable robustness for content security. Practically, due to the introduction of fully trusted model, there is a problem of single point failure. Conventional end-to-end communication also makes it inefficient in practice.

Various existing proposals have been adopted ICN in ICPS application to provide low latency communication. For example, De Silva *et al.* integrated ICN within Internet of things (IoT) to decouple the control plane and the data plane to satisfy the communication requirements of the lighting control. Mick *et al.* [14] suggested an IoT-based ICN on-boarding authentication procedure to handle the data communication. In their approach, the ICN controller was used to key management and centralized server. While this scheme provides a flexible mechanism, it pre-stores a shared key in a physical device, which may significantly undermine its scalability and make data access unfriendly.

Although existing research can ensure some level of access security, those approaches do not fully address in-network caching strategy. This is because most of existing work either happen on a single endpoint or require user to interact with each other. Another concern is that a heavy burden for ICPS devices with limited computational and processing capacities to generate the required signatures with asymmetric cryptography. Additionally, user privacy immediately becomes a paramount task once ICPS devices are connected to the

Internet since the envisioned ICN routers could deduce sensitivity of the message and infer the identities of those who are involved in the message transmission.

Motivated by such observation, the availability of ICN routers allows us to support as an edge cooperative way at the first-hop and last-hop routers in the ICN architecture. As such, exploring a delegation model to the ICPS is a natural solution to reduce computation overhead on ICPS users. To enforce sensor data authenticity and integrity, proxy signature presents a promise to the minimal use of computation overhead on ICPS devices. It allows a proxy to generate a digest of cryptographic on behalf of the original signer. Anyone accessible to the public keys of the original signer and proxy signer can verify the authenticity of the purpoted signature afterwards. Proxy signature can be classified into three delegation types: full delegation, partial delegation and delegation by warrant.

The existing research on proxy signature addresses applications areas different from this article, such as grid computing [8]. There is still few concerns on authentication in ICN ICPS with proxy signature. In this paper, we use proxy signature as a building block to create an authentication framework for ICN ICPS. Our framework ensures that legitimate users to access the authentic sensor data.

2 Problem Statement

2.1 System Model

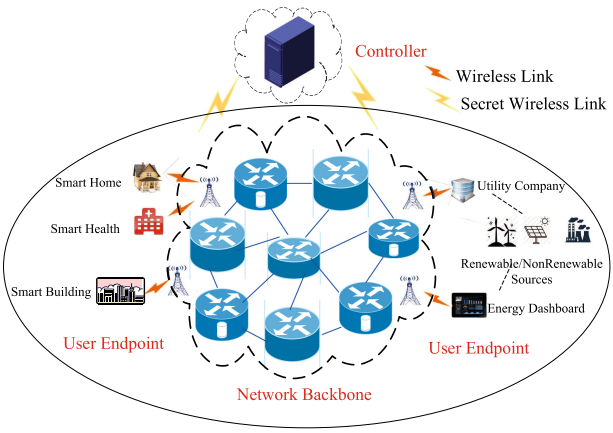

Fig. 1. Two-layer ICN-ICPS architecture.

Figure 1 depicts a basic network architecture of ICN ICPS. The architecture is composed of two levels: the upper level is a controller that provides system infrastructure; the lower level consists of the physical devices, where ICN is leveraged as communication pillar to handle per packet. In the lower level, users use

the two packets types, Interest and Data packets, to communicate and exchange information, respectively. ICN routers as intermediate forwarders are used to do a match between the Interest and Data source, and cache some information to be available for later requests.

There are four types of participants involved in the system, controller, users, edge routers and intermediate routers. In particular, users refer to consumers or ICPS devices who use terminal or application to subscribe or provide the energy service. One of two edge routers, one adjacent to the consumers and another closer to the ICPS devices, to be implemented as edge servers, respectively. We refer to the first edge router as consumer gateway and the second as device proxy. The gateway is enforced access policies to decide whether an interest or data packet should be forwarded or dropped based on the verification results. The proxy is allowed to perform data analysis and then produce certain operations based on the request on behalf of the ICPS devices. Intermediate routers are distributed in the system to forward the packets between users.

2.2 Threat Model

Under the framework shown in Fig. 1, we assume that all participants are registered with a controller, before they are approved to get access the system resource. The controller is not necessarily to be a strong trusted third party. This property makes our model realistic and fine-grind, since a centralized entity necessitates centralized trust and represents a single point of failure. We also assume that there are two types of adversaries: passive adversary and active adversary. Passive attacks may be mounted from the routers who have collected plenty of interests information to learn "who is requesting" and "who is replaying". In contrast the passive adversary, the active adversary has more powerful capabilities so that they could launch some stronger attacks for any packet transmissions at the communication level, such as, capture/analyze interests, modify requests and responds, and also masquerade as legitimate users to send interests.

2.3 Objectives

Our design goal is to propose a secure authentication scheme based on the defined threat model for ICN-ICPS at reasonable cost. For this target, the proposed scheme must hold security attributes. It is desired that the proposed scheme to cover the following requirements:

Integrity: Making sure that the received data is completed, unmodified during transmissions.

Authenticity: Ensuring that the data comes from the ones they claim to be. Any users should be held non-repudiation for their actions.

Authentication: Identifying both users to be adequately trusted and preventing adversaries to mount masquerade attack by performing traffic analysis and capturing packets.

Anonymity: Protecting real identities of the users so that other related privacy information is exposed as little as possible to the intermediate routers.

Key Establishment: Providing a random session key to be contributed by only the user and its responder. This indicates that the negotiated key should be inaccessible to the third party.

Notation: $\mathrm{h}_i(\cdot)$ be hash functions. Q_0, s_0 be system's public key and private key. $Q_\mathrm{A}, s_\mathrm{A}$ be an entity A's public key and private key. id_A be an entity A's identity. $\mathrm{MAC}(\cdot)$ be a message authentication code. $r \leftarrow S$ denotes an element is randomly chosen from the set S. m and σ be a content and its signature. $\mathbb{G}_1$ be a cyclic additive group over prime finite field $\mathbb{F}_p$; $\mathbb{G}_2$ be a cyclic multiplicative group; P be the generator of $\mathbb{G}_1$; q be the prime order of $\mathbb{G}_1$ and $\mathbb{G}_2$; e be a pairing from $\mathbb{G}_1$ to $\mathbb{G}_2$; The Computational Diffie-Hellman (CDH) problem: Given $\langle P, aP, bP\rangle$ with uniformly random choices of $a, b \leftarrow \mathbb{Z}_q^*$, compute $abP \leftarrow \mathbb{G}_1$.

3 Building Block: Proxy Signature

In this section, we propose a proxy signature that relies on non-trusted-aided third party and prove its security is equivalent to the CDH problem in the random oracle model. Then, we analyze the performance in terms of signature size and computation overhead.

3.1 Construction

The proxy signature consists of a `Setup` algorithm, two sub-algorithms `PartialKeyGen` and `KeyGen`, and a proxy designation issuing algorithm which involves three algorithms: `ProxyKeyGen`, `Sign`, and `Verify`.

`Setup`: Algorithm 1 takes security parameter κ and returns the system parameters params and master-key. Generally, this algorithm is run by a carrier called Private Key Generator (PKG). We assume throughout that params are publicly known, while the master-key will be known only to the PKG.

Algorithm 1: `Setup`

Input: 1^κ

Output: s, params= $\langle \mathbb{G}_1, \mathbb{G}_2, e, P, Q_0, \mathrm{h}_1, \mathrm{h}_2, \mathrm{h}_3, \mathrm{h}_4, \mathrm{MAC}\rangle$

1: Generate $\langle \mathbb{G}_1, \mathbb{G}_2, e\rangle$.

2: Choose

$P \leftarrow \mathbb{G}_1$, $s \leftarrow \mathbb{Z}_q^*$, $\mathrm{h}_1, \mathrm{h}_3 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $\mathrm{h}_2, \mathrm{h}_4 : \{0,1\}^* \rightarrow Z_q^*$.

3: Compute $Q_0 \leftarrow sP$.

`PartialKeyGen:` The PKG runs Algorithm 2 to generate a partial key for each entity A. The algorithm inputs params, master-key, a secret value $x_A \leftarrow \mathbb{Z}_q^*$ selected by entity A and an identifier for entity A with a string $id_A \leftarrow \{0,1\}^*$, as input. Each partial private key is calculated by hashing an identity id_A and $x_A P$ to append them with the master-key. Usually, the output is transported to entity A over a confidential channel.

Algorithm 2: `PartialKeyGen`

Input: params, id_A, $x_A P$

Output: p_A corresponding to A

1: Transmit A $\rightarrow$ PKG: $\langle id_A, x_A P \rangle$.

2: Compute

$D_A \leftarrow h_1(id_A, x_A P)$, $p_A \leftarrow s D_A$.

`KeyGen:` Algorithm 3 takes as input params, an entity A's partial private key p_A and A's secret value x_A and constructs A's private key s_A and public key Q_A, respectively. Each full private key is a combination of each partial private key p_A and a secret random value x_A. And a public key is computed by $x_A P$. This algorithm is run by an entity A itself who is the only entity in possession of x_A.

Algorithm 3: `KeyGen`

Input: params, p_A, x_A

Output: s_A/Q_A corresponding to A

1: Compute

$s_A \leftarrow \langle p_A, x_A \rangle$, $Q_A \leftarrow x_A P$.

`ProxyKeyGen:` Algorithm 4 requires only two short communication flows between an original signer and a proxy signer. It begins to run at the original signer side and gets as input params, the original signer's secret value x_A and a warrant m_ω that includes delegation period, message types, the identity information of a proxy signer id_B, the public key of an original signer Q_A and a proxy signer Q_B. The original signer commits itself to a proxy transcript proxy-trans: $\langle m_\omega, \varpi \rangle$ and then transmits them to the proxy signer who is designated to check it using the original signer's public key. Consequently, the proxy signer will get a proxy signing key pair $SK_B \leftarrow \langle x_B, p_B + x_A H_2 P \rangle, PK_B \leftarrow \langle id_B, Q_B \rangle$ if the check is correct.

Algorithm 4: `ProxyKeyGen`

Input: params, x_A, m_ω, Q_A, Q_B

Output: true: $\langle SK_B, PK_B \rangle$; **false:** failure.

1: Compute
$H_2 \leftarrow h_2(id_B, m_\omega, Q_A, Q_B)$, $\varpi \leftarrow \frac{x_A D_B}{x_A + H_2}$.
2: proxy-trans: $\langle m_\omega, \varpi \rangle$.
3: Compute
$H_2 \leftarrow h_2(id_B, m_\omega, Q_A, Q_B)$.
4: Check **if** $e(\varpi, Q_A + H_2 P) = e(Q_A, D_B)$ **then**
5: return **true**
6: **else**
7: return **false**
8: **end if**

`Sign`: Algorithm 5 runs at the proxy side who signs a message m on behalf of the original signer. It requires params, a proxy secret key SK_B, proxy-trans, the public-key of the proxy signer. The resulting signature on the message m consists of the triple $\langle R, V \rangle$.

Algorithm 5: `Sign`

Input: params, SK_B, PK_B, proxy-trans

Output: σ

1: Choose $r \leftarrow \mathbb{Z}_q^*$.
2: Compute
$R \leftarrow rP$, $H_3 \leftarrow h_3(m, id_B, R, Q_B)$,
$V \leftarrow p_B + x_A H_2 P + x_B H_2 P + r H_3$.
3: $\sigma \leftarrow \langle R, V \rangle$.

`Verify`: Algorithm 6 runs at the verifier side and checks the validity of a signature of a given message m with respect to params and a set of public key $\langle PK_B, Q_A \rangle$, respectively. Notice that if σ is a valid signature on a message m, it outputs **true** and **false** otherwise.

3.2 Comparison

We compare signature length and computational complexity with the most recent signature schemes [11,18,20] in Table 1. In Table 1, $\mathbb{G}_1$ and Exp. in signature length represent the size of the group element and modulus, respectively,

Algorithm 6: `Verify`

Input: params, σ, m, Q_{A}, PK_{B}

Output: **true:** success; **false:** failure.

1: Check **if**
$e(V,P) = e(Q_0, D_{\mathrm{B}}) \cdot e(Q_{\mathrm{A}}, H_2P) \cdot e(Q_{\mathrm{B}}, H_2P) \cdot e(R, H_3)$
then
2: return **true**;
3: **else**
4: return **false**;
5: **end if**

and pair. and $\mathbb{G}_1$ in computation denote the computation complexities of a pairing and a group operation. Here we assume that the cost of an exponential computation is equal to that of elliptic curve multiplication.

Table 1. Comparison of signature length and computational complexity of signature protocols

Protocol	Signature Length	Computational Complexity		
		`KeyGen`	`Sign`	`Verify`
Xiong-Qin [18]	$3(\mathbb{G}_1)$	$10(\mathbb{G}_1)$	$8(\mathbb{G}_1)$	$5(\mathrm{Pair}) + 3(\mathbb{G}_1)$
Hwang *et al.* [11]	$3(\mathbb{G}_1) + 5(\mathrm{Exp.})$	$3(\mathbb{G}_1)$	$4(\mathrm{Pair}) + 7(\mathbb{G}_1)$	$6(\mathrm{Pair}) + 5(\mathbb{G}_1)$
Zhang *et al.* [20]	$1(\mathbb{G}_1) + 1(\mathrm{Exp.})$	$4(\mathbb{G}_1)$	$1(\mathbb{G}_1)$	$2(\mathrm{Pair}) + 3(\mathbb{G}_1)$
Ours	$2(\mathbb{G}_1)$	$3(\mathbb{G}_1)$	$5(\mathbb{G}_1)$	$4(\mathrm{Pair}) + 1(\mathbb{G}_1)$

Signature Length: To achieve equivalent secure level, the size of prime p is considered to be at least 512 bits. And for achieving a fair comparison, using a supersingular elliptic curve $y^2 = x^3 + ax$ group $\mathbb{G}_1$ of order q with embedding degree two, a modulus size that satisfying $q|p+1$ for any odd $q = 3(mod)4$. Table 1 summarizes the comparison results. Observe that our signature length is sightly longer than [20] but shorter than [11,18] (i.e., we use the fact that bit length of q with 160 bits and the group element in $\mathbb{G}_1$ with 512 bits). Therefore, the bandwidth consumption on the proposed signature is approximately the same as the state-of-the-art.

Computational Complexity: We compare `KeyGen`, `Sign` and `Verify` algorithms in Table 1 which are the main stages in these schemes. In general, the cost of a pairing operation is several times than a scalar multiplication in $\mathbb{G}_1$. Thus, the number of pairing operations is a key performance metric. Table 1 summarizes the results and omits other operations due to their trivial complexity.

Accordingly, the key generation needs three multiplication operations, the signing operation requires three multiplication operations and no pairing computations. The verifier can collapse the $e(Q_A, H_2P)$ and $e(Q_B, H_2P)$ pairings into a single $e(Q_A + Q_B, H_2P)$ term. Thus verifying a signature requires one multiplication operation and four pairing computations. Observe that our signature only incurs a minor cost than [20] but obviously outperforms signature systems [11,18]. However, it is worth noting that our signature algorithm is secure against forgery attack which lays down a concrete design foundation for the whole scheme.

4 Our Solutions

To satisfy the security demands of ICN-ICPS, the proposed proxy signature as a building block to design authentication scheme, preserving the anonymity of user. We first give a basic overview of our design and then describe it.

4.1 Overview

Our framework presents two techniques: proxy signature and session-based variant, that provides authentication for ICPS traffic. The proxy signature is used to authenticate the claimed providers to their consumers without revealing their actual identities, while the session-based variant aims to verify the legitimacy of the requesting consumer.

A full specification of our scheme consists of five steps: The first step is the registration procedure between entities (users, gateway, and proxy) and the controller which served as the PKG (See `PartialKeyGen` in Sect. 3.1). The second step is performed at the consumer side who initiates an Interest packet, its neighbor gateway forwards the packet to the routers until reaching the ICPS device. The third step is performed at the ICPS device side who delegates its signing rights to a designated proxy (See `ProxyKeyGen` in Sect. 3.1). The fourth step is performed at the proxy side who generates a cryptographic digest of the data on behalf of the ICPS device and returns it to the gateway along the original path (See `Sign` in Sect. 3.1). This step happens at the time that there are no cache hit on router nodes. Upon successful receiving the data packet, the last step is the communication interaction between the consumer and its gateway. The consumer is granted to access the content once its identity is valid (See Sect. 4.2). Figure 2 illustrates the interactions between the users, gateway, routers, and proxy and their corresponding procedure execution.

To summarize, all routers may infer content exchanged using cache, but cannot link cache to a specific user. Our design not only does not require interactions with the provider in existence, but also achieve authentication with no identity information leakage on both users.

4.2 The Complete Authentication Scheme

Prior to beginning the communication, the controller initializes the system and publicizes the system parameters params, both participants need to identify themselves to the controller and acquire a pair of key $\langle Q_{\mathrm{C}}, s_{\mathrm{C}}\rangle$, $\langle Q_{\mathrm{GW}}, s_{\mathrm{GW}}\rangle$, $\langle Q_{\mathrm{EP}}, s_{\mathrm{EP}}\rangle$, $\langle Q_{\mathrm{P}}, s_{\mathrm{P}}\rangle$ for consumer, gateway, edge proxy and provider according to `KeyGen` algorithm described in Sect. 3.1.

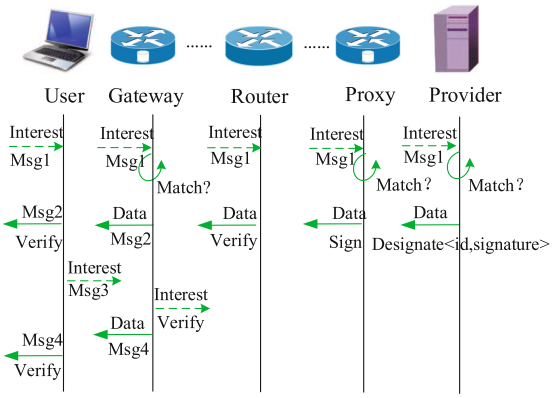

Fig. 2. An overview of our solutions. Here match denotes ICN router checks cache.

Consider a scenario, where a consumer attempts to obtain the power data for different purposes (e.g., real-time energy charging and distribution) from the resource providers (which can be the public administration or a private company). The consumer only intends to receive the valid content without any forging, altering or making a false content. On the other hand, the content is required to be legally consumed to prevent malicious consumers from launching security attacks against legitimate consumers. Table 2 shows the interactions between consumer and its gateway, in which the gateway has privilege of immediately responding to the consumer due to it has the matched content that satisfies the consumer requirements.

A consumer initiates a topic to broadcast its interest Msg1 in its vicinity. Starting from the name root tree [?], / delimits the boundaries of the components. The *domain* indicates that a specific area coverage that a provider entity can offer service. The *energy* specifies the main service that belongs to the provider. The *access* specifies the macro category service that offers further details useful related with the provider to create a more specific answer to the included into the Data. The *query* specifics the consumer demand.

We describe the case when the gateway is trying to achieve a connection with the consumer for the first time. Note that we assume here that the gateway has retrieved a Data packet from the proxy using the Interest paradigm from the network. Generally, this step is carried out when the requested content cannot be satisfied in any routers.

Table 2. Message exchange outline

Msg1:	**Interest:**
	/domain/energy/Access/Query
Msg2:	**Data:**
	Name: */domain/energy/Access/Query*
	Signature Info: $\langle Signature \rangle$
	Content: Session Invite Packet
Msg3:	**Interest:**
	/domain/authenticate/id/Communicate/Req
Msg4:	**Data:**
	Name: */domain/authenticate/id/Communicate/Req*
	Signature Info: $\langle Signature \rangle$
	Content: Response Packet

As mentioned-above, the gateway invites a session by sending an invitation connection Data packet Msg 2 which contains three components of content packets, i.e., name, signature and content itself together with a randomly generated identity *id*, used later by the gateway to identify itself to the consumer. Specifically, the gateway follows Algorithm 7 which outputs a $\langle signature \rangle$ that includes a set of public values with the help input parameters due to the fact that ICN requires every content to be authenticated.

Algorithm 7: Msg2 performed by gateway

Input: params
Output: $\langle Signature \rangle$
1: Choose $r_{\mathrm{GW}} \leftarrow \mathbb{Z}_q^*$.
2: Compute
$U \leftarrow r_{\mathrm{GW}} P$, $W \leftarrow p_{\mathrm{GW}} + r_{\mathrm{GW}} Q_0$.
3: $\langle Signature \rangle : \langle U, W \rangle$.

After obtaining the Data packet within a tolerable time interval, the consumer has to communicate with the nearby gateway to reply a request message to be able to pass the authentication step. The consumer responds with Msg3 by running algorithm 8 that takes the gateway's set of attributes such as public key Q_{GW}, identity *id* and private key s_{C} of the consumer associated with other essential public parameters params as inputs and outputs Req as the components of the reply messages.

The consumer constructs an Interest packet Msg3, where `authenticate` field explicits the sub-categories-of-services that accepts of the invite contains the identity *id* of who it corresponds to the gateway which allows a direct, bi-

directional `communicate` path between them. It then returns the Data packet to the gateway inviting the session.

Algorithm 8: Msg3 performed by user

Input: params, s_{C}, Q_{GW}, $\langle Signature \rangle$

Output: **true:** Req: $\langle E, S \rangle$; **false:** failure.

Check **if** $e(W, P) = e(D_{\mathrm{GW}}, Q_0) \cdot e(U, Q_0)$ **then**
  Pick $r_{\mathrm{C}} \leftarrow \mathbb{Z}_q^*$.
  Compute
  $E \leftarrow r_{\mathrm{C}} Q_{\mathrm{GW}}$, $S \leftarrow r_{\mathrm{U}} P - x_{\mathrm{U}} D_{\mathrm{GW}}$.
  return **true**
else
  return **false**
end if

Algorithm 9 is performed by the gateway when receiving the Interest packet from the invited consumer. After check the equality, the gateway constructs a Data packet Msg4 that includes the content m, and τ encoded in the $\langle signature \rangle$ along with the signature σ together. It returns the Data packet to the consumer requesting the content.

Algorithm 9: Msg4 performed by gateway

Input: params, Req, p_{GW}

Output: **true**: output $\langle Signature \rangle$; **false**: failure

Derive: $r_{\mathrm{C}} P \leftarrow x_{\mathrm{GW}}^{-1} E$,
if $e(p_{\mathrm{GW}}, Q_{\mathrm{C}}) \cdot e(S, Q_0) = e(r_{\mathrm{C}} P, Q_0)$ **then**
Compute
$K \leftarrow \mathrm{h}_4(r_{\mathrm{GW}} P, r_{\mathrm{C}} P,$
$r_{\mathrm{GW}} r_{\mathrm{C}} P)$, $\tau \leftarrow \mathrm{MAC}(r_{\mathrm{GW}} P, K)$.
  return **true**
else
  return **false**
end if

Finally, the consumer executes algorithm 10 with the purpose of verifying the validness of the gateway. If the validation information does not match, the con-

sumer discards the session. Otherwise, the consumer starts to verify the authenticity of the signature originated from the proxy. The consumer rejects the packet if the algorithm outputs false, and accept it otherwise.

Algorithm 10: Msg 4 checked by user

Input: params, σ

Output: **true:** success; **false:** failure

$K' \leftarrow \mathrm{h}_4(r_{\mathrm{GW}}P, r_{\mathrm{C}}P, r_{\mathrm{C}}r_{\mathrm{GW}}P)$
if $(r_{\mathrm{GW}}P, \tau, K') \rightarrow 1$ **then**
    verify σ
    if (verification==successful) **then**
        return **true**
    else
        return **false**
else
    return **false**
end if

5 Security Analysis

5.1 Security Properties Analysis

Our scheme guarantees that the controller only can know partial private keys, avoiding it impersonating as legitimate entity. This policy makes the controller more applicable in real ICN-ICPS scenarios. In what follows, we discuss the authentication scheme with respect to the objectives listed in Sect. 2.3.

Authenticity: An adversary $\mathcal{A}$ cannot forge a signature that is attributed to a legitimate party such that the party cannot repudiate.

Theorem 1. *Suppose hash functions* $\mathrm{h_i}$*(i = 1, 2, 3) are random oracles. If a polynomial time adversary* $\mathcal{A}$ *has an advantage* $\epsilon(\kappa)$ *in forging a signature* σ*, then there exists an algorithm* $\mathcal{C}$ *that can break CDH problem with an advantage at least* $(\epsilon(\kappa)/2)(1 - q_s(q_{\mathrm{h}_3} + q_s)/2^{\kappa})(e(q_{\mathrm{r}} + 1))^{-1}$ *by making* q_{h_3}*,* q_s*,* q_r *queries to the* h_3*, signing and revealpartialkey oracles.*

The security proof can be found in the appendix due to space limitation.

As such, proxy signature ensures that the content contained in the Data packet is valid with respect to the public keys of the proxy and the provider, where different content names can be leveraged to generate different signatures.

Authentication: The issue is mainly twofold. One is to verify the legitimacy of a requesting consumer in case a malicious adversary can launch an impersonation to hurt other innocent consumers' benefits. The other is to check the validity of the provider in case a malicious adversary injects poison content into the system. For the legitimacy of a consumer, only its gateway can authenticate its accessible by comparing $e(p_{\mathrm{GW}}, Q_{\mathrm{C}}) \cdot e(S, Q_0)$ to $e(r_{\mathrm{C}}P, Q_0)$ due to the private key p_{GW} is only known by itself. If it is not valid, any malicious Interest packets from the consumer cannot be verified and will be dropped. For the validity of the provider, we take proxy signature to provide authenticity such that the sign in content indeed originates from the claimed provider. Before that, the gateway is required to be authenticated since frequent content access provided makes it effortless to become the goal of adversaries. Receiving a right τ signals that the gateway is the correct one so that the consumer authenticates the proxy together provider by verifying σ under the public keys of both. The unforgeability guarantee that the system can be convinced that the proxy belongs to its allocated delegation rights.

Anonymity: This property focuses on preventing adversaries from discovering the real identities of both users. In the session-based approach, the real identity of the consumer is only related to its private key which is the result of encryption with the private key of the controller and a random value as inputs. Thus, it is impossible to obtain the real identity due to adversaries have no information about these long-term private keys. Moreover, considering the problem of gateway's compromission, in the communication process of session connection, each consumer can get services without revealing its identity to its gateway. Therefore, if there exists gateway compromised, our scheme can still preserve the privacy of consumers' identities. Preventing adversaries from disclosing the real identity of the provider can be achieved via the proxy signature. Since the provider is anonymous to generate a warrant but tell the proxy nothing on the identity of it. With such approach, adversaries neither know who produces the content nor identify who consumes it. Therefore, identity protection to pair-wise communications is ensured.

Key Establishment: The security of key implies a polynomial time adversary $\mathcal{A}$ cannot distinguish between an instance's real session key and a random value.

Theorem 2. *The authentication scheme* $\prod$ *is secure, assuming the hardness of CDH problem and* h_4 *is a random oracle.*

Proof. Suppose that there exists $p(\kappa)$ participants and $s(\kappa)$ sessions. An oracle $\prod_{i,j}^{t}$ refers to the t-th instance of participant i involved with a partner with j in a session, which has a matching conversation to $\prod_{j,i}^{s}$ with a key as $\mathrm{h}_4(K)$. Define the advantage of $\mathcal{A}$ to be $\epsilon(\kappa)$ and E be that $\mathcal{A}$ can query to the random oracle h_4, here $Pr[\mathcal{A}]$ is the success probability that $\mathcal{A}$ outputs a guess bit $\hat{b}$ such that $\hat{b} = b$ held by one of the oracles $\prod_{i,j}^{t}$. As we know $\Pr[\mathcal{A}] = \Pr[\mathcal{A}|\mathrm{E}]\Pr[\mathrm{E}] + \Pr[\mathcal{A}|\overline{\mathrm{E}}]\Pr[\overline{\mathrm{E}}]$. Note that h_4 is a random oracle and the transcript is part of the input of h_4 to generate the session key, then

$\Pr[\mathcal{A}|\mathrm{E}] = 1/2$. Then, we have $\Pr[\mathcal{A}] \leq (1 + \Pr[\overline{\mathrm{E}}])/2$ and $\Pr[\mathcal{A}] \geq (1 - \Pr[\overline{\mathrm{E}}])/2$. It follows $\Pr[\overline{\mathrm{E}}] \geq 2\epsilon(\kappa)$. That is, $\mathcal{A}$ indeed chose oracle $\prod_{j,i}^{s}$ with a non-negligible advantage $(2\epsilon(\kappa))/(p(\kappa)^2 s(\kappa) q_{\mathrm{h}_4})$, where q_{h_4} denotes the number of h_4 queries. This obviously contradicts to the CDH problem.

5.2 Comparison

The security features among the existing ICN schemes [16,19] are shown in Table 3. In terms of authentication, authenticity, anonymity, with trusted entity, security backbone, with random oracle, our scheme can achieve all of these properties, which cannot be reached by others.

Table 3. Security comparison of our authentication scheme with Xue *et al.* [19] and Nunes-Tsudik [16] schemes

Features	Xue *et al.* [19]	Nunes-Tsudik [16]	Ours
User authentication	√	√	√
Content authenticity			√
Anonymity	Partial		√
Without trusted entity			√
Security assumption	Strong DH		CDH
With random oracle	√		√

√ indicates that the property is satisfied

6 Performance Analysis

To gain insights on the benefits of the proposed scheme, we evaluate the performance of our scheme from the perspectives of efficiency at provider side and overall cost. We use a machine with a two-core 2.70 GHz processor and 8GB memory running Windows 10.0.18362.592 for experiment. For the efficiency at provider side, we compare our scheme with vanilla ICPS (Fig. 3). With vanilla ICPS, signatures are generated by the provider. In contrast, our scheme seamlessly integrates proxy signature that largely alleviates the burden of provider side. For the overall cost, we compare computation and communication overhead with existing ICN-based two-party type schemes [19] and [16] in Table 4. For simplicity, we used a minimal setup containing a single provider, proxy, gateway and consumer in each domain. In Table 4, Pair, G., Enc./Dec., and Mac in computation represent the computation complexities of a pairing, a group operation, a symmetric encryption/decryption and a message authentication code, respectively, and G., Exp., Mac and Enc. in communication denote the size of the group element, modulus, message authentication code and ciphertext.

Efficiency: Define a metric $\eta \leftarrow N_p/N_b$, where N_p and N_b are the number of the most time-consuming operation involved on proxy based model and basic scheme (without proxy), respectively. In the proxy way, signature generation can be further divided into two components: at provider side and at proxy side. Let H_p be the transition probability, then N_p during the time interval, Δt, can be represented by $RN_c\Delta t + H_pN_a\Delta t$, where R is the request arriving rate at provider side, N_c and N_a are the number of the most time-consuming operation needed at provider and proxy, respectively. Note that H_p is also equal to the hit rate because it equates the probability that the content is mismatched by other proxies. Thus, η is represented by $(RN_c + H_pN_a)/(RN_b)$. As shown in Fig. 3, the value H_p increases, the values of η becomes larger because more popular content can be satisfied in the proxy. It makes sense that the gap decreases as the amount of request increases since the increment of signature results in the generation of more content request. That is, more popular content is more favored for our scheme.

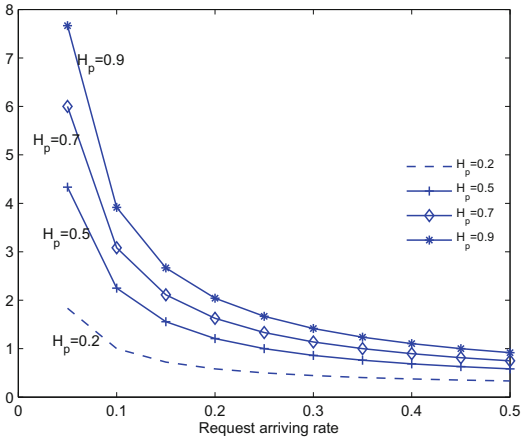

Fig. 3. The value of η with different request arriving rate.

Computation Overhead: Assume that the cost of a symmetric cryptographic computation is equal to that of a Mac computation, and ignore light computations, such as exponential in $\mathbb{Z}_q$, hash and map-to-point hash. Since both the consumer and gateway should check the state of a signature originated by the proxy, the signature verification consumption are considered for measuring the cost of both them. The proposed scheme takes seven pairings, five group operations in $\mathbb{G}_1$, and a Mac operation on average at consumer side, seven pairings, four group operations in $\mathbb{G}_1$ and a Mac operation on average at gateway side, two pairings and five group operations in $\mathbb{G}_1$ on average at proxy side, and one group operation in $\mathbb{G}_1$ on average at provider side. Observe that the computation overhead is more expensive than the competitive one. This degradation is

forgivable since the proposed scheme can offer authentication and anonymity of users simultaneously, which, however, is not the case in the other work.

Communication Overhead: We compute the overall bit size of packets transmitted between users. It comprises seven group elements of $\mathbb{G}_1$ and a Mac. Using the type A elliptic curve described in Sect. 3.2, each element of $\mathbb{Z}_q$, $\mathbb{G}_1$ and $\mathbb{G}_1$ are 160, 512 and 1024 bits, respectively. The comparisons is shown in Table 4. Since our scheme will piggyback signature in Data packets, it will increase the size of communication overheads. However, from Table 4, we can see that the communication complexity of our scheme is higher than [16] but much lower than [19]. A trade-off for perfect authentication security is that both users need to be authenticated, which incurs more communication overhead than [16]. In terms of security features summarized in Table 4, the increased consumption is a substitution for increased security.

Table 4. Performance comparison of our authentication scheme with Xue *et al.* [19] and Nunes-Tsudik [16] schemes

	Xue *et al.* [19]	Nunes-Tsudik [16]	Ours
Computation	**User:** 3(Pair)+9(G.)+1(Dec.) **Gateway:** 5(pair)+8(G.) **Provider:** 2(G.)+1(Enc.)	**User:** 2(Dec.) **Provider:** 4(Enc.)+1(Dec.)	**User:** 7(Pair)+5(G.)+1(Mac) **Gateway:** 7(Pair)+4(G.)+1(Mac) **Proxy:** 2(Pair)+5(G.) **Provider:** 1(G.)
Communication	6(G.)+6(Exp.)+1(Enc.)	5(Enc.)	7(G.)+1(Mac)

7 Conclusion

We present a system framework to enforce security policies in ICN-ICPS such that it can provide end-to-end secure communication. Specially, we incorporate proxy signature to implement a session-based way featured with anonymous authentication. The security of the proposed scheme is proved under the random oracle model. Performance results show that the proposed scheme is an efficient solution that can provide authentication security service for ICN-ICPS user.

Although the proposed scheme tackles some of security problems in ICN-ICPS communication, it is not clear how to deal with the revocation key when users leave or join a topic. Another drawback is that the non-fulfillment of the proposed scheme in a testbed to analyze the performance for system metrics such as latency and energy consumption on user side. Notwithstanding its limitation, the work provides a comprehensive solution for user security in ICN-ICPS. However, these problems might be solved to apply subset difference mechanism and ndnsim and we leave it as future work due to the limitation of the length.

References

1. Cisco annual internet report 2018–2023 white paper. http://www.cisco.com
2. Cyber-physical systems: situation analysis of current trends, technologies, and challenges (2012). http://www.google.com. Accessed 2030
3. Ashibani, Y., Mahmoud, Q.H.: Cyber physical systems security: analysis, challenges and solutions. Comput. Secur. **68**, 81–97 (2017)
4. Azad, M.A., Bag, S., Perera, C., Barhamgi, M., Hao, F.: Authentic-caller: self-enforcing authentication in a next generation network. IEEE Trans. Industr. Inf. **16**(5), 3606–3615 (2020)
5. Chandrasekaran, G., Wang, N., Tafazolli, R.: Caching on the move: towards D2D-based information centric networking for mobile content distribution. In: IEEE 40th conference on Local Computer Networks (LCN), pp. 312–320 (2015)
6. Compagno, A., Conti, M., Droms, R.: OnboardiCNg: a secure protocol for onboarding iot devices in ICN. In: Proceedings of the 3rd ACM Conference on Information-Centric Networking (ICN), pp. 166–175 (2016)
7. Fan, C.I., Chen, I.T., Cheng, C.K., Huang, J.J., Chen, W.T.: FTP-NDN: file transfer protocol based on re-encryption for named data network supporting nondesignated receivers. IEEE Syst. J. **12**(1), 473–484 (2018)
8. Foster, I., Kesselman, C., Tsudik, G., Tuecke, S.: A security architecture for computational grids. In: Proceedings of the 5th ACM Conference on Computer and Communications Security (CCS). pp. 83–92 (1998)
9. Fotiou, N., Polyzos, G.C.: Securing content sharing over ICN. In: Proceedings of the 3rd ACM conference on Information-Centric Networking (ICN), pp. 176–185 (2016)
10. Genge, B., Haller, P., Duka, A.V.: Engineering security-aware control applications for data authentication in smart industrial cyber-physical systems. Future Gener. Comput. Syst. **91**, 206–222 (2019)
11. Hwang, J.Y., Chen, L., Cho, H.S., Nyang, D.: Short dynamic group signature scheme supporting controllable linkability. IEEE Trans. Inf. Forensics Secur. **10**(6), 1109–1124 (2015)
12. Kim, Y., Kolesnikov, V., Thottan, M.: Resilient end-to-end message protection for cyber-physical system communications. IEEE Trans. Smart Grid **9**(4), 2478–2487 (2016)
13. Li, B., Huang, D., Wang, Z., Zhu, Y.: Attribute-based access control for ICN naming scheme. IEEE Trans. Dependable Secure Comput. **15**(2), 194–206 (2016)
14. Mick, T., Tourani, R., Misra, S.: LASeR: lightweight authentication and secured routing for ndn iot in smart cities. IEEE Internet Things J. **5**(2), 755–764 (2017)
15. Misra, S., Tourani, R., Natividad, F., Mick, T., Majd, N.E., Huang, H.: AccConF: an access control framework for leveraging in-network cached data in the ICN-enabled wireless edge. IEEE Trans. Dependable Secure Comput. **16**(1), 5–17 (2017)
16. Nunes, I.O., Tsudik, G.: KRB-CCN: lightweight authentication and access control for private content-centric networks. In: Preneel, B., Vercauteren, F. (eds.) ACNS 2018. LNCS, vol. 10892, pp. 598–615. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93387-0_31
17. Tramarin, F., Vitturi, S., Luvisotto, M.: A dynamic rate selection algorithm for IEEE 802.11 industrial wireless LAN. IEEE Trans. Ind. Inf. **13**(2), 846–855 (2016)
18. Xiong, H., Qin, Z.: Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE Trans. Inf. Forensics Secur. **10**(7), 1442–1455 (2015)

19. Xue, K., Zhang, X., Xia, Q., Wei, D.S., Yue, H., Wu, F.: SEAF: a secure, efficient and accountable access control framework for information centric networking. In: 2018 International Conference on Computer Communications(INFOCOM), pp. 2213–2221. IEEE (2018)
20. Zhang, Y., Deng, R., Zheng, D., Li, J., Wu, P., Cao, J.: Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT. IEEE Trans. Industr. Inf. **15**(9), 5099–5108 (2019)
21. Zheng, Q., Li, Q., Azgin, A., Weng, J.: Data verification in information-centric networking with efficient revocable certificateless signature. In: 2017 IEEE Conference on Communications and Network Security (CNS), pp. 1–9 (2017)