Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6603754, 9 pages
https://doi.org/10.1155/2022/6603754

Research Article

A Remote Attestation Mechanism Using a Threshold Ring Signature for a Perception Layer of Distributed Networking

Jing Huang[1,2] **Jia Chen**[1,2] **Hui-Juan Zhang**[1,2] **Zhe-Yuan Sun**[1,2] **and Shen He**[1,2]

[1]*Research Institute of China Mobile Communications Corporation, Beijing 100032, China*
[2]*Research Institute of Safety Technology, Beijing 100032, China*

Correspondence should be addressed to Jia Chen; chenjia.work@foxmail.com

Received 26 July 2021; Revised 12 November 2021; Accepted 27 December 2021; Published 22 January 2022

Academic Editor: Bithas Petros

Due to the emergence of various new technologies, Internet of things (IoT) is gradually becoming one of the most valued technologies at present. The IoT makes our life more and more convenient through the interconnection of everything, but the IoT brings many advantages and also raises some security issues, such as the IoT perception layer as the main means of sensing data delivery, due to the limited resources of sensing nodes and their vulnerability, the diversity of sensing data, and the heterogeneity of the sensing network, making the IoT perception layer more vulnerable to various malicious attacks. Therefore, guaranteeing the trustworthy source of sensing data is the cornerstone to guarantee the secure operation of the sensing layer. In this paper, we investigate the remote proof scheme applicable to the IoT perception layer and propose a remote attestation mechanism using a threshold ring signature for a perception layer of distributed networking, which realizes the trusted proof of a data source and thus can effectively discern the trusted status of the data source, and prove that the proposed scheme in this paper outperforms other remote proof schemes through efficiency analysis and verify the correctness as well as the effectiveness of the scheme in this paper.

1. Introduction

The Internet is the "bridge" between the real world and the information world [1]; in the age of interconnection, there are tens of thousands of equipment for information interaction moment-by-moment [2]. As the kernel of the IoT, the perception layer is mainly responsible for the acquisition and transmission of massive interaction information.

An IoT sensing network is a wireless self-organized network formed by a large number of sensing nodes. The main function of the Internet of things perception network is to perceive and collect relevant information in a certain area and to distribute and transmit the collected information through collaborative transmission between nodes. The nodes in the perception network can be divided into ordinary perception nodes, data aggregation nodes, and management nodes according to their different functions [3]. Among them, ordinary sensing nodes are mainly responsible for collecting and transmitting environmental data in the area. The data aggregation node summarizes the data collected by the sensing node and performs certain calculation processing. The management node makes a unified judgment and identification on the data collected by the sink node through a certain strategy. Generally speaking, the data processing ability of the sensor node is weak, but it should have a certain information perception ability. The data aggregation node should have stronger data processing and storage capabilities. The management node is connected to the data aggregation node through an external network and performs application control on the sensing network.

On the one hand, the Internet of things perception network is similar to traditional networks in terms of networking and communication methods. On the other hand, it also has many characteristics that traditional networks do not have. It can complete functions that traditional networks cannot do, but at the same time, these characteristics also bring many security problems to the perception network. The characteristics of the sensing network of the Internet of things are as follows: sensing network nodes being distributed in a wide area, sensing network dynamic adaptability

needs, and sensing network node resources being limited. Because the communication of the sensing layer node is easily eavesdropped and the resources are limited, it is not suitable for some highly complex cryptographic algorithms; with the evolution of attack methods, the sensing node is facing a huge security risk. Once the sensing node is destroyed, being controlled by criminals will cause the loss and tampering of important data, resulting in irreparable losses. The security issues facing the perception layer of the Internet of things include the following: node malicious control, illegal information capture, network DoS attacks, and counterfeiting attacks; e.g., in October 2016, a massive network outage occurred on the East Coast of the U.S., which was caused by a DDoS attack launched by a camera acting as a broiler [4], so it is an urgent issue to ensure the reliability of the perception nodes [5]. Currently, to cope with the security problems of the perception layer network, the most important issues in the operation of IoT are the security of nodes and confidentiality and integrity of data, and usually we use password mechanisms, authentication, intrusion detection, etc. to secure the network.

At present, remote attestation technology is an important technique for establishing trusted relationships between entities in distributed computing environments [6]. In the direction of proving the state of the perception node platform, the Trusted Computing Group (TCG) proposed a binary remote proof scheme by combining the characteristics of integrity metrics and trusted computing trust chains [7]. The binary remote attestation scheme mainly relies on trusted third parties and uses the trusted third parties to store the standard metric values of trusted platforms. However, how to ensure the reliability of the third party is the main bottleneck. International Business Machines (IBM) Corporation implemented a prototype system for direct attestation of a perception node state using the binary remote proof approach [8], which meets the remote attestation requirements of TCG specification. Nevertheless, this proposed prototype system by IBM suffers from platform configuration exposure.

In summary, the simple remote proof scheme described above uses the metric as the state flag of the system; however, this mechanism has some problems, such as management difficulties due to the complexity and volatility of the system and security problems caused by the digital signature of the AIK as a metric. The TCG-based remote proof mechanism also suffers from the inability to perform dynamic proofs and the inability to resist the use of the AIK as the digital signature of the metric and to resist replay attacks.

2. Related Work

In order to solve these problems in the TCG remote proof mechanism, scholars at home and abroad have conducted further in-depth research on remote proofs, such as semantic-based remote proof schemes and attribute-based remote proof schemes, but attribute-based remote proofs still have some defects, such as coarse granularity of attributes, large complexity of attribute mapping, and difficulty of attribute revocation. The literature [9] proposes a trusted proof mechanism based on attribute certificates, with the help of abstracting the attributes commonly owned by computing platforms into certificates containing these attributes; thus, privacy exposure problems can be effectively avoided, and the efficiency of the whole proof process can be improved. Attribute-based proof (PBA) schemes are proposed in the literature [10], which are more manageable than the hash-based proofs proposed in the TCG specification and also provide platform-specific techniques for integrity and identity authentication; although these solutions propose remote authentication and auditing schemes, they are not yet perfect and are not fully applicable to the current state of the IoT perception layer. The literature [11] proposes a fine-grained attribute-based remote proof mechanism that can accurately portray the security attributes of a platform and is resistant to forgery attacks; however, it is slightly less computationally efficient in terms of the computational efficiency of component attribute proofs, especially for the presence of a large number of components. To overcome the drawbacks of TCG-based remote proof mechanisms, a large number of hybrid remote authentication models have been proposed [12]. The literature [13] proposes a semantic remote authentication model that combines remote proofs with virtual technologies and proposes a complex remote authentication model using language-based virtual machine technology with dynamicity as well as platform independence. The literature [14] proposes a ring signature-based remote proof scheme for attribute configuration that solves the problem of platform configuration leakage in binary proofs, but the scheme adds attribute configuration lists and the mapping of security attributes and configurations in attribute proofs is intractable; also, the update of configuration lists is not efficient. The literature [15] proposed a remote automatic anonymous proof scheme based on trusted computing technology, which achieves the purpose of anonymous proof and protection of its own privacy through ring signature and can effectively avoid the leakage of privacy, but the scheme does not accurately abstract the external platform attribute values from the external attribute certificates. The literature [16] proposed an efficient cluster remote proof mechanism applicable to IoT based on grouping of sensing nodes, by grouping IoT devices to set up management nodes for cluster remote proof represented by management nodes, which has high security against collusion attacks. The literature [17] proposes an automatic audit as well as proof mechanism (FoNAC) for fog nodes to secure the fog layer, FoNAC uses the Trusted Platform Module (TPM 2.0) feature to evaluate and audit the platform integrity of running fog nodes and grant certificates to each fog node after successful security audits, and this scheme can resist replay attacks, forgery attacks, and distributed denial-of-service attacks (DDoS).

Therefore, in order to improve the self-adaptive capability and guarantee the anonymity of nodes, a remote attestation mechanism using a threshold ring signature (TRS-TRS) for the perception layer of distributed networking is proposed in this paper. The main contributions of this paper are as follows.

(1) A remote attestation mechanism (RAM), based on the ring signature of the computational Diffie-Hellman (CDH) problem, is established for the perception layer nodes in distributed networking

(2) A TRS strategy is proposed for the perception nodes in different logical groups to identify the trusted state of data sources and guarantee the privacy exposure of perception nodes

(3) The security properties of the proposed TRS-RAM, including the correctness, unconditional anonymity, and unforgeability, are tested to reveal its effectiveness

3. Preliminary

3.1. Ring Signature. A ring signature allows users to sign in the name of a self-organizing group of users (called a ring) without revealing the identity of the signer. The concept of the ring signature is similar to that of a group signature, which both hides the identity of the signer to a group. However, they are significant differences. The group administrator in the group signature scheme can revoke the anonymity of the group signature, while the group in the ring signature can select and hide the identity of the signer and does not need for any collaboration among users, due to no centralized authority in ring signatures. Therefore, ring signatures can provide higher anonymity and are more suitable for decentralized application scenarios [18].

The ring signature consists of three processes: keygen, sign, and verify. Let the public key sequence $R = (pk_1, \cdots, pk_n)$ be a ring and $R_{[i]} = pk_i$; the formal definition of the ring signature is as follows:

(1) $(pk, sk) \longleftarrow \text{KeyGen}(1^\lambda)$. The key generation algorithm takes the security parameter $\lambda \in N$ as the input and the public-private key pair (pk, sk) of the user as the output

(2) $\sigma \longleftarrow \text{Sign}(sk, s, M, R)$. The signature algorithm takes the user private key sk, location s, message M, and ring R as input and outputs the signature σ, where $(R_{[s]}, sk)$ is a pair of keys output by the key generation algorithm, and R contains more than two public keys and two are different

(3) $b \longleftarrow \text{Verify}(R, M, \sigma)$. The verification algorithm takes the ring R, the message M, and the signature σ as input and outputs the verification result of message M under the ring R

3.2. Bilinear Mapping. Define $G_1 = <g_1>$ and $G_2 = <g_2>$ to be multiplicative cyclic groups of order p, p to be a prime number, g_1 and g_2 to be generators of G_1 and G_2, respectively, and $e : G_1 \times G_1 \longrightarrow G_2$ to be a computable mapping that is a bilinear mapping if it satisfies the following properties.

(1) Bilinear: there is a mapping $e : G_1 \times G_1 \longrightarrow G_2$ making all $\alpha \in G_1, \beta \in G_2, \forall x, y \in Z$ and exists $e(\alpha^x, \beta^y) = e(\alpha, \beta)^{xy}$

(2) Nondegeneracy: there exist $g_1 \in G_1$, $g_2 \in G_2$, and $e(g_1, g_2) \neq 1$

(3) Computability: for $\forall \alpha \in G_1, \forall \beta \in G_2$, there exists an efficient algorithm to compute $e(g_1, g_2)$

3.3. CDH Problem. Given the group of $G = <g>$, known g, g_a, g_b, and $a, b \in Z_p$, it is difficult to compute g^{ab}, when a, b are unknown.

4. A Remote Attestation Mechanism Using the Threshold Ring Signature

In this proposed TRS-RAM, first, the perception node can be divided into several logical groups to eliminate the untrustworthy nodes by the trusted metric model and logic grouping. Then, when the perception node needs remote attestation to the external environment, the remote node can be informed of the logical group to which the perception node belongs and cannot trace the real node itself, due to the different logical groups each having different trustworthiness. Based on the above analysis, the proposed TRS-RAM consists of three parts: credibility metric of perception node, trusted logic grouping, and RAM. The specific process is shown in Figure 1.

(1) Credibility metric of perception node: the aggregation node at the regional boundary performs the credit metrics on the perception nodes within the comprehensive metrics, combining the static credibility metrics, dynamic credibility metrics, subjective direct trust, and objective recommendation trust of the perception node

(2) Trusted logic grouping: some perception nodes with similar characteristics can be divided into a trusted group through the trustworthiness logic grouping mechanism. Then, when a node needs to prove to the outside world, it only proves that the perception node belongs to a trusted group, so that its identity and location privacy are not exposed

(3) RAM: the perception nodes are usually managed by the aggregation nodes. Therefore, the perception nodes in different logical groups can sign their trustworthiness information using the TRS strategy. Then, the remote nodes can analyze and judge whether the data source is trustworthy based on the signature verification results. If the data source is abnormal, the remote nodes can refuse interaction to achieve unconditional anonymity and unforgeability

Remark 1. Compared with some security mechanisms, the proposed TRS-RAM can efficiently evaluate the credibility of the data source node to ensure that interaction information is more secure and meanwhile guarantee the anonymity of node identity.

4.1. Construction of TRS-RAM. This part describes the signature parameter establishment, signature, and verification of the TRS-RAM scheme. Choose the large prime cyclic group G of order P with $G_T, e : G \times G \longrightarrow G_T$ as a bilinear mapping. Specify that $H_u : \{0,1\}^* \longrightarrow \{0,1\}^n{}_u$ and H_m

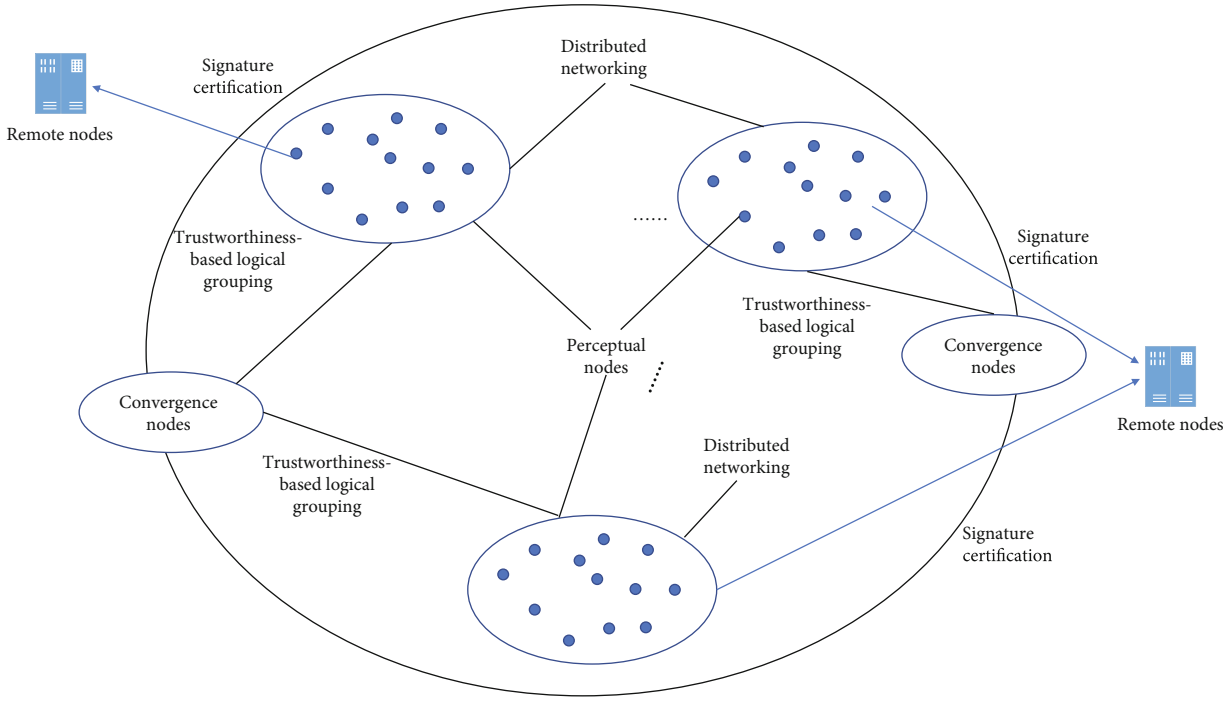

Figure 1: The scheme of the proposed TRS-RAM.

$: \{0,1\}^* \longrightarrow \{0,1\}^n{}_m$ are both secure hash functions in which the bit number of the node unique identification ID and information m is the bit vector of n_u and n_m. The construction of TRS-RAM is as follows:

4.1.1. The Signature Parameter Establishment of TRS-RAM. Choose arbitrarily $\alpha \in Z_p$, g_2, u', $m' \in G_1$, n_u, and n_m, Z_p is an integer domain, g is a generating element of G, and u_i and m_i are the number of bit vectors. $g_1 = g^a$, $\widehat{U} = (u_i)$, and $\widehat{M} = (m_i)$; $\widehat{U}$ is the bit vector of u_i, and $\widehat{M}$ is the bit vector of m_i. For arbitrarily choosing $u_i, m_i \in G$, the system master key is $ga\,2$ and the relevant parameters are $(G, G_r, e, g, g_1, g_2, u', \widehat{U}, m', \widehat{M}, H_u, H_m)$.

The perception node is identified as ID, let $u = H_u(\mathrm{ID})$ be the bit vector of n_u, and $\Phi_u \subseteq \{1, 2, 3, \cdots, n_u\}$ is the ith list with $u_{[i]} = 1$. For randomly selecting random number $r_u \in Z_p$, the private key of the node identifier corresponding to ID is

$$d_{\mathrm{ID}} = (d_1, d_2) = \left(g_2^a \left(u' \prod_{i \in \Phi u} u_i\right), g^{r_u}\right). \tag{1}$$

4.1.2. The Signature Process of TRS-RAM. When the system parameters are established, the signature node will sign for the message m (message m is the credibility of the perception node). For the n perception nodes $\{\mathrm{ID}_1, \mathrm{ID}_2, \mathrm{ID}_3, \cdots, \mathrm{ID}_n\}$ in a certain perception layer, the signature identification list of the t $(t < n)$ nodes is $\{\mathrm{ID}_1, \mathrm{ID}_2, \mathrm{ID}_3, \cdots, \mathrm{ID}_t\}$ and the signature identification list of remaining nodes is $\{\mathrm{ID}_{t+1}, \mathrm{ID}_{t+2}, \cdots, \mathrm{ID}_n\}$; the signature process is as follows:

(1) The signature node ID_i arbitrarily chooses $s_i \in Z * p$ and sets s_i as the secret parameter. Then, the signature node ID_i $(i = 1, 2, \cdots, t)$ chooses the polynomial $f_i(x)$:

$$f_i(x) = a_{i,0} + a_{i,1}x + \cdots + a_{i,t-1}x^{t-1}. \tag{2}$$

Let $S_i = a_{i,0}$, and each ID_i gets

$$C_{i,d} = g^{a_{i,d}} (d = 0, 1, \cdots, t-1), \tag{3}$$

where $C_{i,d}$ can be shared with other signature nodes and $s_{i,j} = f_i(j)$. Then, $s_{i,j}$ is shared with all nodes except itself (all other members in the signature subset), and record $s_{i,i} = f_i(i)$ for itself.

(2) The node ID_j gets the $s_{i,j}$ broadcasted by ID_i, and if the left and right sides of equation (4) are equal:

$$g^{s_{i,j}} = \prod_{d=0}^{t-1} \left(C_{i,d}{}^{jd}\right), \tag{4}$$

the verification is successful.

(3) The secret of every node ID_i is

$$x_i = \sum_{j=1}^{t} s_{j,i}. \tag{5}$$

(4) In the set of signature nodes $\{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_t\}$, the private key of the signature node ID_i is $(d_{i,1}, d_{i,2})$. $M = H_m(L, m, t)$ and $M \subseteq \{1, 2, \cdots, n_m\}$ are the list of the bit vectors $M_m = 1$ of m:

$$\begin{aligned}\sigma_i &= \left(d_{i,1}\left(m'\prod_{k\in M} m_k\right)^{x_i\eta_i}, d_{i,2}, g^{x_i\eta_i}\right)\\ &= \left(g_2^{\alpha}\left(u'\prod_{k\in \Phi IDi} u_k\right)^{r^{\mathrm{ID}_i}}\left(m'\prod_{l\in M} m_l\right)^{x_i\eta_i}, g^{r^{\mathrm{ID}_i}}, g^{x_i\eta_i}\right)\\ &= (\sigma_{i1}, \sigma_{i2}, \sigma_{i3}),\end{aligned}$$

$$\eta_i = \prod_{j=1, j\neq i}^{t} \frac{j}{j-i} \bmod p, \tag{6}$$

where η_i is the Lagrangian coefficient.

(5) At each node in the set, for arbitrarily choosing r_1, $r_2, \cdots, r_n \in Z_p$, let

$$U_i = u'\prod_{j\in \Phi \mathrm{ID}_i} u_j, i = 1, 2, 3, \cdots, n. \tag{7}$$

Thus, σ can obtain

$$\sigma = \left(\prod_{i=1}^{t}\sigma_{i1}\left(\prod_{i=1}^{n}(U_i)^{r_i}\right), \sigma_{12}g^{r_1}, \cdots, \sigma_{t2}g^{r_t}, g^{r_{t+1}}, \cdots, g^{r_n}, \prod_{i=1}^{t}\sigma_{i3}, \sum_{i=1}^{t} f_i(x)\right). \tag{8}$$

(6) The final TRS of message m and the list of nodes $\{\mathrm{ID}_1, \mathrm{ID}_2, \mathrm{ID}_3, \cdots, \mathrm{ID}_n\}$ is $\sigma = (V, R_1, \cdots, R_n, R_m, f)$

4.1.3. Verification of TRS-RAM. The remote node can check $\sigma = (V, R_1, \cdots, R_n, R_m, f)$ to determine the exception. There are no less than t signed nodes to jointly verify that the generation process of $\sigma = (V, R_1, \cdots, R_n, R_m, f)$ is in the list of nodes $\{\mathrm{ID}_1, \mathrm{ID}_2, \mathrm{ID}_3, \cdots, \mathrm{ID}_n\}$.

(1) The remote node verifies the error number of f and then checks whether R_m is equal to $g^{f(0)}$. If it is equal, the remote node continues the following verification process and vice versa; otherwise, it means that the verification is not successful

(2) Then, the remote node judges

$$e(V, g) = e(g_1, g_2)e(U_1, R_1)\cdots e(U_n, R_n)e\left(m'\prod_{l\in M} m_l, R_m\right). \tag{9}$$

If the equation is satisfied, it means that $\sigma = (V, R_1, \cdots, R_n, R_m, f)$ is legitimate and the signature can be accepted; otherwise, the signature is rejected.

4.2. Security Analysis of TRS-RAM. To ensure the security of the proposed TRS-RAM, the correctness, anonymity, and unforgeability can be verified.

(1) Correctness

Theorem 1. *Assuming that all the perception nodes in the set $\{ID_1, ID_2, ID_3, \cdots, ID_n\}$ can faithfully execute the signature protocol, the signer can correctly generate a signature for message m. Accordingly, the verifier must also be able to verify it successfully.*

Proof. In the proposed TRS-RAM, considering that

$$\sum_{i=1}^{t} x_i\eta_i = f(0) = \sum_{i=1}^{t} f_i(0) = \sum_{i=1}^{t} s_i, \tag{10}$$

thus

$$R_m = \prod_{i=1}^{t}\sigma_{i3} = g^{\sum_{i=1}^{t} x_i\eta_i} = g^{f(0)}. \tag{11}$$

□ □

The signature σ is calculated:

$$\begin{aligned}e(V, g) &= e\left(\prod_{i=1}^{t}\sigma_{i1}\left(\prod_{i=1}^{t}(U_i)^{r_i}\right), g\right)\\ &= e\left(g_1, g_2^{t\alpha}\right)e\left((U_1)^{r_{\mathrm{ID}_1}+r_1}\cdots(U_t)^{r_{\mathrm{ID}_i}+r_i}(U_{t+1})^{r_{t+1}}\cdots(U_n)^{r_n}\left(m'\prod_{l\in M} m_l\right)^{\sum_{i=1}^{t} x_i\eta_i}, g\right)\\ &= e(g_1, g_2)^t e\left((U_1, g)^{r_{\mathrm{ID}_1}+r_1}\cdots e(U_n, g)^{r_n}e\left(\left(m'\prod_{l\in M} m_l\right), g\right)\right)^{\sum_{i=1}^{t} x_i\eta_i}\\ &= e(g_1, g_2)^t e\left((U_1, R_1)\cdots e(U_n, R_n)e\left(\left(m'\prod_{l\in M} m_l\right), R_m\right)\right).\end{aligned} \tag{12}$$

From equation (12), it is clear from the above proof process that as long as the signer generates the signature correctly according to the signature protocol, the signer can get a legitimate signature; Theorem 1 is proven.

(2) Anonymity

Theorem 2. *The proposed TRS-RAM has unconditional anonymity; i.e., for the TRS generated by the set of nodes $\{ID_1, ID_2, ID_3, \cdots, ID_n\}$, the probability that an attacker can successfully guess is less than 1/d and thus has unconditional anonymity.*

Proof. Considering that

$$f(x) = \sum_{i=1}^{t} f_i(x), \tag{13}$$

where $f(x)$ is obtained randomly by the set of nodes $\{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_i, \cdots, \mathrm{ID}_t\}$, thus the private secret x_i of the signature node is irregular. Moreover, $R_{t+1}, \cdots, R_n, R_m$ in the signature σ are also irregular and cannot expose the relevant features of the real signature node. For R_i and V:

$$R_i = g^{r_{\mathrm{ID}_i} + r_i},$$
$$V = g_2^{ta}(U_1)^{r_{\mathrm{ID}_1}+r_1} \cdots (U_t)^{r_{\mathrm{ID}_i}+r_i}(U_{t+1})^{r_{t+1}} \cdots (U_n)^{r_n}\left(m' \prod_{l \in M} m_t\right)^{f(0)}, \tag{14}$$

where g_2^a represents the master key, $R_i\,(i = 1, 2, \cdots, t)$ is irregular and the selection of $(r_{\mathrm{ID}_1} + r_1, \cdots, r_{\mathrm{ID}_t} + r_t, \cdots, r_{t+1}, \cdots, r_n, f(0))$ is also chosen irregularly; thus, they are not associated with the real signature node.□ □

Therefore, assuming that the attacker has unlimited computational power and can intercept the private keys of all signature nodes in $\{\mathrm{ID}_1, \mathrm{ID}_2, \mathrm{ID}_3, \cdots, \mathrm{ID}_n\}$ at the same time, the probability that the attacker can successfully guess the actual subset of signatures is no more than $1/d$ in terms of probability; i.e., the attacker cannot trace the subset of signatures in $\{\mathrm{ID}_1, \mathrm{ID}_2, \mathrm{ID}_3, \cdots, \mathrm{ID}_n\}$ for a subset of signatures. Therefore, the proposed TRS-RAM satisfies unconditional anonymity. Theorem 2 is proven.

(3) Unforgeability

Theorem 3. *By taking the CDH hard problem as a premise, this signature process is unforgeable. Only the specified nodes can produce a correct signature, and the exceptional node or a subset of group node cannot produce a correct signature.*

Proof. If attacker A can forge the legitimate signature subset with nonnegligible probability, an algorithm B which is a probabilistic polynomial can be constructed. A can solve the CDH hard problem by invoking B with ζ probability in time t.□ □

B is the A certain CDH instance (g, g^a, g^b) of the presupposed, and it is desired to solve the CDH hard problem by A and subsequently obtain g^{ab}, so that B impersonates the challenger of A. It can be divided into various steps as follows.

(1) System initialization. Let $l_{u+} = 2(q_e + q_s)$ and $l_m = 2q_s$, q_e represents the number of queries of the private key, and q_s represents the number of signature key queries which is queried by A. The $k_u\,(0 \le k_u \le n_u)$ and $k_m\,(0 \le k_m \le n_m)$ are arbitrarily selected. $l_u(n_u + 1)$ and $l_m(n_m + 1)$ are less than p. $x' \in Z_{lu}$ is randomly picked and $X = (x_i)$ whose bit number is n_u, and x_i belongs to Z_{lu}; $z' \in Z_{lm}$ is randomly picked by B and $Z = (z_k)$ whose bit number is n_m, and x_i belongs to Z_{lu}; $x' \in Z_{lu}$is randomly picked by$B$ and $X = (x_i)$ whose bit number is n_u, and z_k belongs to Z_{lm}; y' is randomly picked by B and $Y = (y_i)$ whose bit number is n_u, and y_i belongs to Z_p; and w' is randomly picked by B and $W = (w_i)$ whose bit number is n_m, and w_i belongs to Z_p

For the bit vector $u = H_u(\mathrm{ID})$ and $M = H_m(L, m, t)$ which are the bit vector of unique identification ID in the perception node list L and signature message, it is specified as follows:

$$\begin{cases} F(\mathrm{ID}) = x' + \sum_{i \in \Phi} x_i - l_u k_u, \\ J(\mathrm{ID}) = y' + \sum_{i \in \Phi} y_i, \\ K(M) = z' + \sum_{i \in M} z_i - l_m k_m, \\ L(M) = w' + \sum_{i \in M} w_i. \end{cases} \tag{15}$$

For the proposed TRS-RAM, B can use the parameters:

$$\begin{cases} g_1 = g^a, g_2 = g^b, \\ u' = g_2^{-l_u k_u + x'} g^{y'}, m' = g_2^{-l_m k_m + z'} g^{w'}, \\ u_i = g_2^{x_i} g^{y_i} (1 \le i \le n_u), \\ m_i = g_2^{z_i} g^{w_i} (1 \le i \le n_m). \end{cases} \tag{16}$$

There is no difference between the parameters in equation (16) and the public parameters derived by the attacker. Therefore, $ga2 = g^{ab}$ and

$$\begin{aligned} u' \prod_{i \in \Phi u} u_i &= g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})}, \\ m' \prod_{i \in M} m_k &= g_2^{K(m)} g^{L(m)}, \end{aligned} \tag{17}$$

where B can transfer these parameters to A.

(2) Query. If A makes a query, B will make a reply. The query can be divided into private key query and signature query

Private key query: when A interrogates the private key of node ID_u, even though B cannot know its master key, B can also compute that the private key of node ID_u is d_{ID_u}, assuming that $F(\mathrm{ID}_i) \neq 0 \mod p$. B randomly selects $r_u \in Z_p$ and

then yields

$$d_{\mathrm{ID}_u} = (d_{u1}, d_{u2}) = \left(g_1^{-J(\mathrm{ID})/F(\mathrm{ID})} \left(u' \prod_{i \in \Phi u} u_i \right)^{r_u}, g_1^{-1/F(\mathrm{ID})} g^{r_u} \right),$$
$$\tilde{r}_u = r_u - \frac{\alpha}{F(\mathrm{ID})}. \tag{18}$$

Thus, it can know that d_{ID_u} is the legal private key of the node identification ID_u.

$$\begin{aligned} d_{u1} &= g_1^{-\frac{J(\mathrm{ID})}{F(\mathrm{ID})}} \left(u' \prod_{i \in \Phi u} u_i \right)^{r_u} \\ &= g_2^a \left(g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})} \right)^{-a/F(\mathrm{ID})} \left(g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})} \right)^{r_u} \\ &= g_2^a \left(g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})} \right)^{r_u - (a/F(\mathrm{ID}))} = g_2^a \left(u' \prod_{i \in \Phi u} u_i \right)^{r_u}, \end{aligned}$$

$$d_{u2} = g_1^{-1/F(\mathrm{ID})} g^{r_u} = g^{r_u - a/F(\mathrm{ID})} = g r_u. \tag{19}$$

For A, the private key constructed by B is exactly the same as the private key generated by the real challenger. If $F(u) = 0 \bmod p$, the above process cannot continue and B cannot succeed.

Signature query: first, B needs to compute $M = H_m(L, m, t)$ and then obtains the $\mathrm{TRS}(t, n)$ by the following procedure:

(a) B arbitrarily selects $s, a_0, a_1, \cdots, a_{t-1} \in Z_p$ and sets the $(t-1)$th polynomial $f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$, $s = a_0$

(b) The list $L = \{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$ has no less than t I $\mathrm{D}_i, i \in (1, 2, \cdots, n)$ to make that $F(\mathrm{ID}_i) \neq 0 \bmod p$. Assume γ is the set which makes the $F(\mathrm{ID}_i) \neq 0 \bmod p$ hold. Then, $\gamma = (1, 2, \cdots, t)$. B can calculate the private key based on the process of private key query, and then, the private secret $x_i = f(i)$ of all nodes $\mathrm{ID}_i = (1, 2, \cdots, t)$ that perform TRS can be derived. The corresponding gated-ring signature is constructed by the proposed TRS-RAM based on the signature generation process

If the number of nodes in list L which makes $F(\mathrm{ID}_i) \neq 0 \bmod p$ is less than t, B can construct a TRS. Let $K(M) \neq 0 \bmod p$. Then, B arbitrarily picks $r_1, \cdots, r_n, r_m \in Z_p$ and can obtain

$$\begin{aligned} \sigma &= \left(\left(\prod_{i=1}^{n} (U_i)^{r_i} \right) g_1^{-tL(M)/K(M)} \left(m' \prod_{k \in M} m_k \right)^{r_m}, g^{r_1} \cdots, g^{r_n}, g_1^{-t/K(M)}, g^{r_m}, f(x) \right) \\ &= \left(g_2^{ta} \left(\prod_{i=1}^{n} (U_i)^{r_i} \right) \left(m' \prod_{k \in M} m_k \right)^{r_m}, g^{r_1} \cdots, g^{r_n}, g^{r_m}, f(x) \right), \end{aligned}$$

$$r_m = r_m - \frac{ta}{K(M)}. \tag{20}$$

Thus, σ is valid. If $K(M) = 0 \bmod p$, then the above process will stop and B fails.

(3) Forgery. For $L^* = \{\mathrm{ID} * 1, \cdots, \mathrm{ID} * n\}$, A can forge the signature σ^* of TRS for m^* and threshold value t. B can verify

$$F(\mathrm{ID}_i^*) = 0 \bmod p, i \in (1, \cdots, n), \tag{21}$$

$$K(M_i^*) = 0 \bmod p, M_i^* = H_m(L, m^*, t), \tag{22}$$

where equations (21) and (22) are not satisfied; B cannot be successful. If both equations are satisfied, B yields

$$\begin{aligned} &\left(\frac{V}{R_1^{J(\mathrm{ID}_1^*)} \cdots R_n^{J(\mathrm{ID}_n^*)} R_m^{L(M^*)}} \right)^{1/t} \\ &= \left(\frac{g_2^{ta} \left(u' \prod_{i \in \Phi_1} u_i \right)^{r_1} \cdots \left(u' \prod_{i \in \Phi n} u_i \right)^{r_1} \left(m' \prod_{k \in M} m_j \right)^{r_m}}{g^{J(\mathrm{ID}_1^*) r_1} \cdots g^{J(\mathrm{ID}_n^*) r_n} g^{L(M^*) r_m}} \right)^{1/t} \\ &= \left(g_2^{ta} \right)^{1/t} = g_2^a = g^{ab}, \end{aligned} \tag{23}$$

where the result is the answer to the difficult question. Therefore, if the probability of an attacker succeeding in forging a legitimate gated-ring signature is nonnegligible, there must be a corresponding algorithm to solve the hard problem. However, this contradicts the assumptions of the discrete logarithm problem. Theorem 3 is proven that the proposed TRS-RAM in this paper is known to be unforgeable.

In summary, for the perception layer distributed networking model, the (t, n) threshold ring signature scheme based on node trusted logical grouping designed in this section under the standard model realizes the trusted proof of the data source, and by analyzing and proving the security of the scheme, it is known that the scheme can effectively protect the privacy information of the proof nodes, has unconditional anonymity, and satisfies the unforgeability, while the signature of the scheme length is short; therefore, the proposed scheme in this paper is secure, efficient, and suitable for perceptive nodes with limited computational resources.

Remark 2. Based on the above analysis, for the distributed networking model of the perception layer, the proposed TRS-RAM can realize the credibility attestation of perception nodes. Moreover, it can be seen that this proposed TRS-RAM can effectively protect the privacy information and has the correctness, unforgeability, and anonymity by analyzing the security of TRS-RAM.

Table 1: Comparison of time complexity of various operations.

Computational	Time complexity
Scalar multiplication operation S	$1S \approx 29$ M
The addition of points A	$1A \approx 0.11$ M
The bilinear pair operation P	$1P \approx 87$ M
Exponential operation E	$1E \approx 21$ M
Ordinary hashing operation h	Neglect

Table 2: Calculation of the impact of offloading on the signature scheme.

Options	Computational complexity	Total time spent	Times
Solution [20]	$1S + 1E$	$1S + 1E \approx 50$ M	0.0975 s
Solution [21]	$2S + 1E$	$2S + 1E \approx 79$ M	0.15405 s
Our solution	$3S + 1H$	$3S + 1H \approx 87$ M	0.16965 s

Meanwhile, the group signature length of TRS-RAM is short. Therefore, the proposed TRS-RAM in this paper is secure and efficient and more suitable for perception nodes with limited computational resources.

5. Efficiency Analysis

Table 1 shows the time complexity of each operation, comparing the data with the literature reference [19]. Considering the smart terminal with the latest CortexA9 1.2 GHz microprocessor, the time of the quantitative multiplication operation on the elliptic curve is about 0.00195 s. Combining Table 1 with Table 2, it can be seen that the scheme in this section is more efficient than all the existing comparison schemes.

6. Conclusions

In this paper, a TRS-RAM was designed to evaluate the credibility of the perception node and protect the autologous identity privacy. The remote attestation process can be accomplished by introducing TRS, which can avoid exposing the privacy of the node. The verifying node can inquire the credibility of the perception node from the management node based on the received signature and can also trace the node when the data is disputed to achieve the dynamic tracking of the node. Moreover, the proposed TRS-RAM has the correctness, unforgeability, and anonymity to effectively guarantee the security of the perception node, and our solution has higher efficiency compared to others. In our future work, some improved TRS mechanisms will be studied for perception nodes to further improve the certification performance.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] D. Georgakopoulos and P. P. Jayaraman, "Internet of things: from internet scale sensing to smart services," *Computing*, vol. 98, no. 10, pp. 1041–1058, 2016.

[2] D. Wang and J. Zhao, "A new approach to heterogeneous wireless sensor networks reliability evaluation based on perception layer in Internet of vehicles," *Photonic Network Communications*, vol. 37, no. 2, pp. 179–186, 2019.

[3] X. Li, Z. Xuan, and L. Wen, "Research on the architecture of trusted security system based on the Internet of things," in *In 2011 Fourth International Conference on Intelligent Computation Technology and Automation*, vol. 2, pp. 1172–1175, 2011.

[4] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[5] O. Vermesan, P. Friess, P. Guillemin et al., "Internet of things strategic research roadmap, cluster of European research projects on the Internet of things," in *CERP-IoT*, 2011.

[6] Y. Ning, Y. Zhu, R. C. Wang, R. Malekian, and Q. M. Lin, "An efficient authentication and access control scheme for perception layer of Internet of things," *Applied Mathematics & Information Sciences*, vol. 8, no. 4, pp. 1617–1824, 2014.

[7] R. Sailer, X. Zhang, and T. Jaeger, "Design and implementation of a TCG-based integrity measurement architecture," in *Proc. of the 13th Conf. on USENIX Security Symp*, 2004.

[8] R. Sailer, V. L. Doorn, and J. P. Ward, "The role of TPM in enterprise security," in RC23363 (W0410-029), IBM Research, 2004.

[9] J. Zhao, Z. Han, J. Liu, and R. Zhang, "A remote proof protocol based on trusted cryptographic module," *Journal of Beijing Jiaotong University*, vol. 34, no. 2, pp. 33–37, 2010.

[10] A. Awad, S. Kadry, B. Lee, and S. Zhang, "Property based attestation for a secure cloud monitoring system," in *IEEE/ACM 7th International Conference on Utility and Cloud Computing*, pp. 934–940, IEEE, 2014.

[11] Y. Qin and D. Feng, "Component property based remote attestation," *Journal of Software*, vol. 20, no. 6, pp. 1625–1641, 2009.

[12] V. Haldar, D. Chandra, and M. Franz, "Semantic remote attestation: a virtual machine directed approach to trusted computing," *USENIX Virtual Machine Research and Technology Symposium.*, vol. 2004, 2004.

[13] L. Zhu, Z. Zhang, L. Liao, and C. Guo, "A secure robust integrity reporting protocol of trusted computing for remote attestation under fully adaptive party corruptions," in *Future Wireless Networks and Information Systems*, pp. 211–217, Springer, Berlin, Heidelberg, 2012.

[14] X. Zhang, X. Y. Yang, and R. R. Zhu, "A remote proof scheme for attribute configuration based on ring signature," *Journal of Wuhan University: Science Edition*, vol. 2, pp. 117–121, 2016.

[15] J. Q. Liu, J. Zhao, and Y. Zhao, "A study of remote automatic anonymous proofs in trusted computing," *Journal of Computer Science*, vol. 32, no. 7, pp. 1304–1310, 2009.

[16] B. Du, Y. Qin, W. Feng, and X. Chu, "An efficient cluster proof mechanism for the Internet of things," *Computer Systems Applications*, vol. 27, no. 10, pp. 22–32, 2018.

[17] M. Aslam, B. Mohsin, A. Nasir, and S. Raza, "FoNAC - an automated fog node audit and certification scheme," *Computers & Security*, vol. 93, p. 101759, 2020.

[18] S. Balaji, "Secure data sharing in cloud without certificate verification process using ID-based proxy ring signature," *Data Mining and Knowledge Engineering*, vol. 8, no. 4, pp. 1304–1310, 2006.

[19] S. H. Islam and G. P. Biswas, "A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks," *Annals of télécommunications-annales des telecommunications*, vol. 67, no. 11-12, pp. 547–558, 2012.

[20] F. Hess, "Efficient identity based signature schemes based on pairings," Springer-Verlag, Berlin, 2003, SAC'2002,LNCS 2595.

[21] H. Yoon, J. Cheon, and Y. Kim, "Batch verifications with ID-based signatures," Springer-Verlag, Berlin, 2005, ICISC'2004, LNCS 3e506.