sensors

MDPI

Article

Fuzzy-Based Privacy-Preserving Scheme of Low Consumption and High Effectiveness for IoTs: A Repeated Game Model

Laicheng Cao * and Min Zhu

School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China; zhumin_lut@163.com

* Correspondence: caolch@lut.edu.cn

Abstract: In the Internet of things (IoTs), data transmission via network coding is highly vulnerable to intra-generation and inter-generation pollution attacks. To mitigate such attacks, some resource-intensive privacy-preserving schemes have been adopted in the previous literature. In order to balance resource consumption and data-privacy-preserving issues, a novel fuzzy-based privacy-preserving scheme is proposed. Our scheme is constructed on a T-S fuzzy trust theory, and network coding data streams are routed in optimal clusters formulated by a designed repeated game model to defend against pollution attacks. In particular, the security of our scheme relies on the hardness of the discrete logarithm. Then, we prove that the designed repeated game model has a subgame-perfect Nash equilibrium, and the model can improve resource utilization efficiency under the condition of data security. Simulation results show that the running time of the proposed privacy-preserving scheme is less than 1 s and the remaining energy is higher than 4 J when the length of packets is greater than 400 and the number of iterations is 100. Therefore, our scheme has higher time and energy efficiency than those of previous studies. In addition, the effective trust cluster formulation scheme (ETCFS) can formulate an optimal cluster more quickly under a kind of camouflage attack.

Keywords: fuzzy trust; repeated game; pollution attacks; camouflage attack; optimal cluster; ETCFS

Citation: Cao, L.; Zhu, M. Fuzzy-Based Privacy-Preserving Scheme of Low Consumption and High Effectiveness for IoTs: A Repeated Game Model. *Sensors* **2022**, *22*, 5674. https://doi.org/10.3390/s22155674

Academic Editors: Weizhi Meng and Xiaobo Ma

Received: 16 June 2022
Accepted: 26 July 2022
Published: 29 July 2022

1. Introduction

The Internet of things (IoTs) refers to the networked connection of all daily objects, which can play an eminent role in the application of services based on the Internet of things, such as intelligent fire protection, industrial monitoring, intelligence collection, renewable energy adaptation, and so on, greatly simplifying and bringing convenience to life [1,2]. However, IoT is vulnerable to various network attacks, which can destroy the process of data transmission and increase energy consumption. Therefore, in the previous literature, many privacy-preserving schemes have been proposed to protect the security of data. Furthermore, network coding technology has been introduced into IoTs for protecting the privacy of data, where the sensor data is divided into multiple generations. Specifically, the multiple packets in any generation are signed by an identifier. With this kind of packet mixing, characteristic of the network coding, an internal or external enemy can inject some fake or modified packets into the information flow, making it more vulnerable to contamination attack, so that IoT devices cannot identify the correct and trusted data. In addition, the polluted data will spread widely. In response to network-coding-enabled IoT attack scenarios, we consider two typical types of pollution attacks. We firstly consider intra-generation attacks, where the attacker modifies the innocent packets in multiple generations. Secondly, we consider inter-generation attacks, where the attacker forges the malicious packets into valid packets in one generation. In contrast with previous defense works, we introduce a T-S fuzzy trust evaluation model to defend against malicious IoT devices and construct an energy-efficient privacy-preserving framework. In the T-S fuzzy trust evaluation model, limited bandwidth and power consumption are considered. Meanwhile,

our T-S fuzzy trust model can obtain a more accurate trust evaluation value under the premise of ensuring the required stability of IoTs. Referring to [3–5], we design a repeated game model to perfect the energy-efficient privacy-preserving scheme, where the subgame Nash equilibrium of the repeated game model can balance the data security and network resource consumption [6]. The contributions of this research are given as follows:

- Firstly, we propose a novel privacy-preserving scheme based on T-S fuzzy trust theory to mitigate the pollution attacks, in which the security is proved according to the hardness of the discrete logarithm.
- Secondly, we construct a repeated game model to formulate the optimal cluster, in which subgame-perfect Nash equilibrium is achieved, and the energy efficiency is higher than in previous research under a kind of camouflage attack.
- Finally, we prove the correctness of our privacy-preserving scheme through strict mathematical derivation and verify the performance superiority of our scheme by simulation.

The organization of this paper is as follows. In Section 2, we present the previous theories, including privacy-preserving schemes, T-S fuzzy technology, and the game theory on which this research is based. In addition, we present a variety of improved models adapted to coding trust in IoTs and discuss the shortcomings of these works in Section 3. After that, we propose the energy-efficient privacy-preserving scheme based on the T-S fuzzy trust model and repeated game model in Section 4. Then, the simulation results and discussion are provided in Section 5, proving the correctness and accuracy of our proposed model. Finally, we draw our conclusions in Section 6.

2. Related Works

2.1. Privacy-Preserving Schemes

At present, the technologies to solve pollution attacks in network coding can be roughly divided into two categories: information theory schemes and cryptography-based schemes. The information theory scheme mainly prevents pollution attacks by detecting and correcting the polluted packets on the sink node. Regarding the effectiveness of information theory methods, they cannot make intermediate nodes filter out fake messages, which means that they can only passively tolerate the pollution attacks of sink nodes.

Another solution to the problem of pollution attacks is password-based authentication technology that enables transponders to verify the accuracy of packets they receive in routing. This method enables intermediate nodes to detect and discard fraudulent packets in transmission, which can effectively reduce pollution attacks from the source [7].

In [8], a homomorphic signature scheme based on the hardness of the discrete logarithm problem was proposed, which allows a node to check the validity of a packet without decoding it. In this scheme, the node can check the integrity of the received packet by taking advantage of the linearity of the packet in the coding system. In addition, Zhang et al. [9] proposed a new idea called "orthogonal fill" in network coding, combining a signature scheme based on public keys with a MAC scheme based on symmetric keys. This scheme requires updating the public-private key tuple, which results in a high cost of forwarder calculation. Liu and Wang in [10] divided pollution attacks in actual network coding into intra-generation pollution attacks and inter-generation pollution attacks. Each packet of each generation depends on the correct identifier and the corresponding dynamic public key designed for this generation for validation. The scheme works by shuffling static keys, and each shuffling is only used in one generation. However, the scheme only focuses on the prevention of pollution attacks in general.

Besides the authentication scheme based on the asymmetric key, there is also a class of authentication schemes based on symmetric key encryption. To solve the problem of label contamination, Li et al. in [11] proposed a time-based authentication scheme called RIPPLE, which uses delayed MAC key disclosure to achieve security similar to public key authentication schemes. It is the first scheme to consider tag contamination, allowing nodes to effectively detect corrupted packets and encode only validated packets. Cheng and Jiang

proposed a homomorphic message authentication code scheme for network coding in [12], which they claimed could obtain a reliable security parameter.

Although the authentication scheme based on the symmetric key has lower computational complexity than that based on the asymmetric key, it still has large bandwidth overhead and key management problems. In [13], Cheng et al. proposed two improved key distribution schemes for, respectively, signature schemes based on homomorphic subspace and label-encoding schemes based on key pre-allocation, which can reduce the homomorphism of messages belonging to two different generations to combat multi-generation pollution attacks; however, their communication costs increase significantly. In [14], Li et al. proposed a multi-source homomorphic network coding signature in the standard model to deal with multi-source devices in an IoTs network system, to ensure network availability while mitigating pollution attacks. In [15], Fiandrotti et al. propose a simple and effective method to deal with contamination attacks in point-to-point flow based on network coding. The scheme can reduce the impact of pollution attacks by selectively combining the packets of the forwarder and proving that the probability of the packet being drawn increases with time. Subsequently, in [16], Antonopoulos et al. introduced a cooperative nonparametric statistical framework to identify and mitigate node misconduct in IoT coding scenarios. The framework does not require monitoring of wireless channels and additional overhead, but it is not resistant to eavesdropping attacks. In [17], Lawrence et al. proposed a scheme based on homomorphic message authentication coding in IoTs that could identify contamination attacks and attack initiating nodes and developed data/message and marker error correction techniques. In addition, Sodhro et al. included cognitive/brainwaves via electroencephalogram (EEG), which function as a unique performance indicator to construct an energy-efficient cognitive authentication scheme [18] for smart healthcare applications, promoting the development of biometric recognition.

2.2. T-S Fuzzy

Nonlinearity is a common feature of many real systems [19,20]. It is also an important factor that directly leads to the complexity of system analysis and design. Fortunately, the "universal approval" of the Takagi–Sugeno (T-S) fuzzy model can solve the problems caused by nonlinearity well. Therefore, in the past few years, many studies have modeled nonlinear systems as T-S fuzzy systems, which are locally linear time-invariant systems connected by if-then rules. Consequently, studies on T-S fuzzy systems have attracted more and more attention [21]. Various meaningful studies on T-S fuzzy systems have been carried out. To avoid the deterioration of system performance, fault-tolerant control (FTC) and fault detection and isolation (FDI) schemes based on the T-S fuzzy model are developed in [22]. By using the set theory description of the T-S fuzzy model, aiming at the problem of fault isolation of the T-S fuzzy system, a new fault isolation method was proposed in [23], which does not introduce the measurement information of the fault isolation sensor into the premise variables of the corresponding observer. A new descriptor fuzzy sliding-mode observer approach was proposed in [24], which augments the original fuzzy plant into a descriptor system to estimate the system state, sensor fault, and actuator fault vectors at the same time.

In [25], the problem of the hybrid-triggered controller design with quantization was investigated for a T–S fuzzy system under cyber-attacks. However, in practical applications, parameter uncertainties in membership functions are usually inevitable. This has encouraged research on the sliding mode control problem of interval type-2 (IT2) fuzzy systems subject to the unmeasurable state and cyber-attacks by introducing two weighting factors [26]. In [27], by designing a fault detection observer and separating the measured premise variables explicitly from the unmeasurable ones, the finite frequency error detection problem of T-S fuzzy systems with some unmeasurable premise variables was studied.

2.3. Game Theory

The methods of using game theory to mitigate different threats to the security of the Internet of things are broadly summarized, and these methods are classified into cooperative games and non-cooperative games [28]. In addition, some potential research trends with great promising prospects in game theory have been proposed. In [29], a privacy protection solution in an intelligent transportation environment was presented based on a game model consisting of two participants (data holder and data requester). Markov chains were utilized to model transformations for finding the optimal protection strategy for data holders to keep data private over a series of interactions with the data requester. Furthermore, the characteristics of the Stackelberg game are used to model security in IoT applications [30]. At the same time, the Stackelberg game has also been extended to deal with false injected data of intelligent attacks in sensor networks to enhance data trustworthiness [31]. A repeated game model was also presented to enhance the resistance of the Internet of things to selective forwarding attacks [32]. More specifically, in this game, the credibility of high-priority data was maximized by detecting malicious nodes that discard high-priority packets. However, the model attaches too much importance to high-priority packets, which leads to the rapid degradation of low-priority packets due to the impact of unprocessed attacks. Then, cooperative game theory was used to improve security and manage cost and delay, focusing on the trust evaluation process based on mixed-strategy Nash equilibrium [33]. In [29], a repeated game model was proposed to detect and mitigate the influence of malicious cluster members, and a TDMA protocol was adopted to keep the synchronization of cluster heads and cluster members, to reduce the complexity of the detection mechanism.

3. System Model

3.1. Network Model

In this paper, a linear network coding enabling IoT is considered, in which an IoT device sends a batch of sequenced messages to multiple target nodes. The delivered messages are divided into M generations, where each message can be regarded as an n-dimensional vector over the finite field $\mathbb{F}_p$. Here, p is a pre-determined prime integer. Meanwhile, each generation contains m native messages. Without loss of generality, the i-th generation is labeled by an ρ-bit binary string $Id_i \in \{0,1\}^\rho$, where $i \in \{1,\ldots,M\}$ and $\rho \geq \left\lceil \log_2^M \right\rceil$. Let $\Gamma = \{Id_1,\ldots,Id_M\}$ represent the set of generation identifiers. Then, the set of native messages belonging to the i-th generation is defined as $\{\boldsymbol{D}_{i,1},\ldots,\boldsymbol{D}_{i,m}\}$, where

$$\boldsymbol{D}_{i,j} = (\boldsymbol{D}_{i,j}^{(1)},\ldots,\boldsymbol{D}_{i,j}^{(n)}) \in \mathbb{F}_p^n, j \in \{1,\ldots,m\} \tag{1}$$

In this network model, the trust $\boldsymbol{T}$ between IoT devices is considered. The trusted routing device set in the next round of data transmission is selected by the trust value generated in the previous round of data transmission.

3.1.1. Trust Encoding at Data

For the j-th native messages $\boldsymbol{D}_{i,j}$ in the i-th generation, a t-dimensional unit vector $\boldsymbol{p}_j$, with the j-th entry being the measurable trustworthiness $T_{i,j}$ for IoT devices and the other being 0, is appended into the native messages. Then, the corresponding augmented block $c_{i,j}$ is given as follows:

$$\boldsymbol{c}_{i,j} = (\boldsymbol{p}_j, \boldsymbol{D}_{i,j}) = (\overbrace{\underbrace{0,\ldots,0}_{j-1}, T_{i,j}, \underbrace{0,\ldots,0}_{t-j}}^{t}, \boldsymbol{D}_{i,j}) \in F_p^{t+n}, j \in \{1,\ldots,t\}, \tag{2}$$

according to the bi-linear map polynomial-time algorithm, the corresponding encrypted block is given by

$$\begin{aligned} \boldsymbol{E}_{i,j} &= Encrypt(h, Id_i, \boldsymbol{c}_{i,j}) \\ &= (\overbrace{\underbrace{0, \ldots, 0}_{j-1}, e_{T_{i,j}}, \underbrace{0, \ldots, 0}_{t-j}}^{t}, \boldsymbol{D}_{i,j}), \end{aligned} \tag{3}$$

where h is the parameter in the bi-liner map between two multiplicative cyclic groups, and Id_i is the number of IoT devices.

3.1.2. Trust Decoding for Receivers

When the network controller receives the encoding data, the data block is first decrypted and stored in the buffer. After receiving m non-linearly correlated data blocks, the network controller can recover the native messages by Gaussian elimination. Then, an ACK message will be fed back to the sender to confirm the transmission of the next generation of messages.

3.2. Adversary Model

We assume that there exists an attacker attempting to launch attacks in this network. The types of attacks are listed as follows:

- **Pollution attack:** Attackers attempt to launch malicious data injection attacks to disrupt the data transmission. Then, data integrity and privacy are compromised.
- **Camouflage attack**: Attackers deceive their surrounding trust evaluation devices by pretending to be the normal devices, which leads to the wrong trust measurement results.

3.3. T-S Fuzzy Trust Model

Here, the data-privacy-preserving model between IoT devices is introduced. However, we should also consider routing security issues in data transmission. With the development of trust evaluation technology in routing security, Li et al. [34] studied the trust routing model instead of the traditional cryptographic scheme to defend against malicious nodes in IoTs. In practical applications of IoTs, the degree of trustworthiness between IoT devices is usually complex and variable. In this section, we reasonably assume a T-S fuzzy model to mitigate the influence of subjective factors in trust evaluation. The T-S fuzzy model is defined as follows:

Definition 1. *Suppose that the domain* $\boldsymbol{X} = \{x_1, x_2, \ldots, x_n\}$ *is a non-empty set, and* $x_i (i = 1, 2, \ldots, n)$ *is an element in* $\boldsymbol{X}$*. For* $\forall x_i \in \boldsymbol{X}$*, there is a mapping relation as follows:* $\mu_T : \boldsymbol{X} \to [0, 1], x_i \mapsto \mu_T(x_i) \in [0, 1]$*; then, the set* $\boldsymbol{T} = \{(x_1|\mu_T(x_1)), (x_2|\mu_T(x_2)), \ldots, (x_n|\mu_T(x_n))\}$ *is defined as a fuzzy subset* $(\forall x_i \in \boldsymbol{X})$ *on* $\boldsymbol{X}_{\mu_T(x_i)}$*, which is called the membership degree of* x_i *to fuzzy subset* $\boldsymbol{T}$*, and the mapping* μ_T *is called the membership function of fuzzy subset* $\boldsymbol{T}$*.*

In Definition 1, $\boldsymbol{X} = \{x_1, x_2, \ldots, x_n\}$ is the set of IoT devices. Here, we chose the communication trust T_c and energy trust T_e as the fuzzy characters z_k to objectively describe the trustworthiness of IoT devices. Therefore, the vector $v(x_{ji}) = v_{ji} = (\mu_{1i}, \mu_{2i}, \ldots, \mu_{mi})$ formed by the membership degree of each subject competing for these finite fuzzy parameters z_k is used as the evaluation trust vector of $\mu_{ji} \in [0, 1], (j = 1, 2, \ldots, l)$ for x_i, while v_{ji} is the evaluation trust vector of node j to node i, and $\mu_{ki} (k = 1, 2, \ldots, m)$ is the membership degree of node $i(x_i)$ to fuzzy parameter z_k evaluated by node j. Then, the definition of the fuzzy rule is given as follows:

Definition 2. *IF* v_{1i} *is* $\boldsymbol{X}_{\mu_T(1,x_i)}$ *and* v_{2i} *is* $\boldsymbol{X}_{\mu_T(2,x_i)}, \ldots,$ v_{ji} *is* $\boldsymbol{X}_{\mu_T(j,x_i)}$, *THEN*

$$\begin{aligned} \dot{x}(t) &= A_{i_1 i_2 \ldots i_p} x(t) + B_{i_1 i_2 \ldots i_p}(\mu(t) + a_1(t)) + B_w n(t) \\ y^{j_1}(t) &= C^{j_2} x(t), j_1 = 1, \ldots, m-h \\ y^{j_2}(t) &= C^{j_2} x(t) + a_2^{j_2}(t), j_2 = m-h+1, \ldots, m, \end{aligned} \tag{4}$$

Where $x(t) \in \mathbb{R}^n$ is the network statement, $\mu(t) \in \mathbb{R}^l$ denotes the map input, $n(t)$ is the bias of noise, $a_1(t) \in \mathbb{R}^l$ is the attack intensity in network, $a_2(t) \in \mathbb{R}^l$ is the transmission bias for indirect trust evaluation, and $y^{j_1}(t) \in \mathbb{R}$ and $y^{j_2}(t) \in \mathbb{R}$ are respectively the output of direct and indirect trustworthiness in the T-S fuzzy model. In addition, m is the number of IoT devices within two hops of node x_i, and h is the number of IoT devices that can communicate directly with node x_i. Then, C is the measurable trustworthiness including communication trust C_1 and energy trust C_2, while $A_{i_1 i_2 \ldots i_p}$, $B_{i_1 i_2 \ldots i_p}$, and B_w are known matrices with suitable dimensions. Then, the $y(t)$ and C can be rewritten as follows,

$$y(t) = \begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix}, C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}, \tag{5}$$

Then, a singleton fuzzifier inference method with center average defuzzifiers is applied to rewrite the T-S fuzzy model as follows:

$$\begin{aligned} \dot{x}(t) =& \frac{1}{\sum_{i_1=1}^{r_1} \sum_{i_2=1}^{r_2} \cdots \sum_{i_p=1}^{r_p} \left(\prod_{j=1}^{p} \boldsymbol{X}_{\mu_T(1,x_i)} \right)} \\ & \times \sum_{i_1=1}^{r_1} \sum_{i_2=1}^{r_2} \cdots \sum_{i_p=1}^{r_p} \left(\prod_{j=1}^{p} \boldsymbol{X}_{\mu_T(1,x_i)} \right) \\ & \times \left(A_{i_{1\to p}} x(t) + B_{i_{1\to p}}(\mu(t) + a_1(t)) + B_w n \right) \\ y(t) =& Cx(t) + a_2(t). \end{aligned} \tag{6}$$

Therefore, we can obtain the objective T-S fuzzy set $\boldsymbol{T} = \{y(1), y(2), \ldots, y(t)\}$, $1 \leq t \leq n$.

4. The Energy-Efficient Privacy-Preserving Scheme Based on T-S Fuzzy Trust Model and Repeated Game Model

In this section, we introduce the framework of our privacy-preserving scheme. Figure 1 shows the relationship between fuzzy trust evaluation, the repeated game model, and the trust privacy-preserving scheme, in which the repeated game helps the network controller formulate the optimal cluster to send the data to the trust privacy-preserving scheme. The game model can obtain a balance between network performance and resource consumption so that we can ensure maximum network performance by consuming fewer resources. Here, network performance indicators include defense attack capability, energy consumption, and so on. Explanations of this can be found in [35]. Therefore, the IoT data can be safely transmitted with low energy consumption.

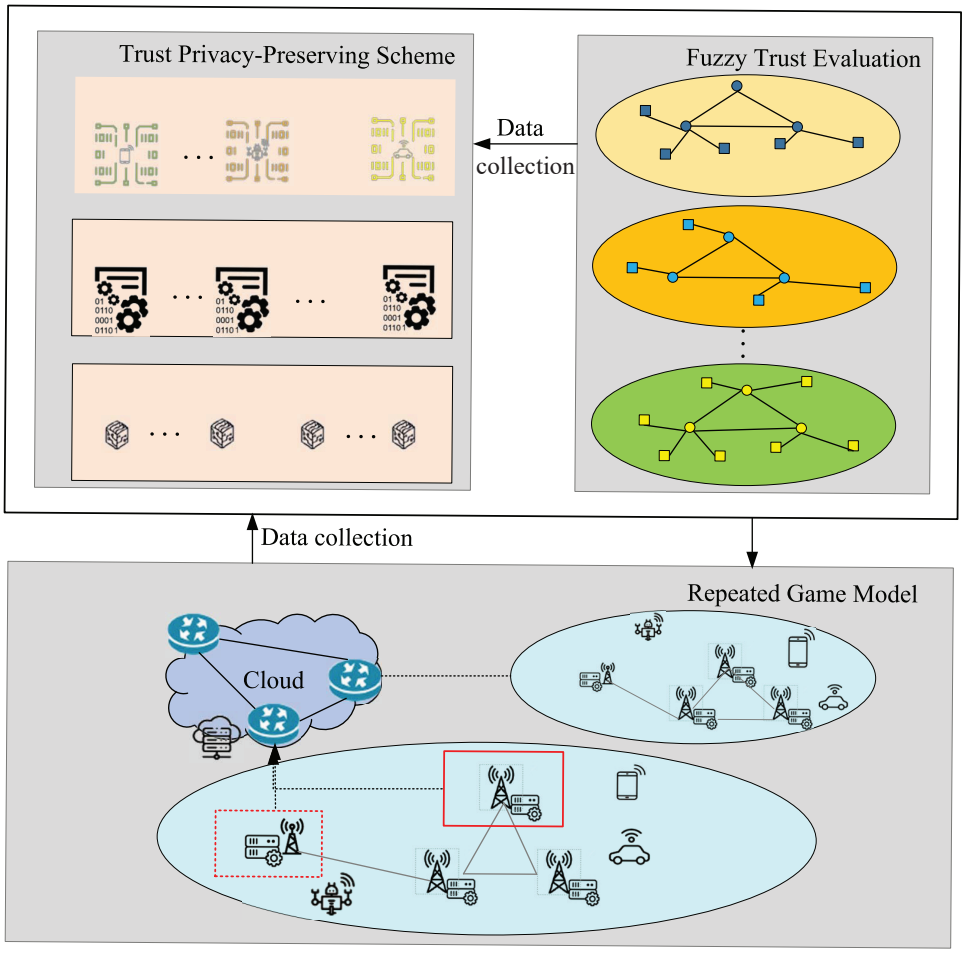

Figure 1. The framework of the fuzzy-based privacy-preserving scheme based on the repeated game. The devices in the solid line frame are common IoT devices in the cluster, and the dotted line is the routing device that guarantees data uploading.

4.1. A Privacy-Preserving Scheme Based on T-S Fuzzy Trust Model

In this subsection, we propose a privacy-preserving scheme based on the T-S fuzzy model, which can protect data privacy against pollution attacks in coding IoT networks. Firstly, the scheme can be formulated as four steps (**Encrypt** , **Sign**, **Verify**, **Decrypt**). The details of those steps are given as follows:

- **Encrypt** (h, $\boldsymbol{T}$, Id_i $\boldsymbol{c}$). According to Definition 1, the trust set $\boldsymbol{T}$ contains 0 and 1. When the trustworthiness of IoT devices is 1, the coding data will be received. Then, the source is generated as a series of t-bit binary strings $\{s_j\}_{j=1}^{t}$. A keyed pseudo-random function $f : \{0,1\}^* \times \{0,1\}^* \times \mathcal{K} \mapsto \mathbb{F}_p$ is applied to generate the encryption matrix

$$\boldsymbol{E}_{\boldsymbol{c},\boldsymbol{T}} = \begin{bmatrix} c_{e_{i,1}} & & \\ & \ddots & \\ & & c_{e_{i,t}} \end{bmatrix}. \tag{7}$$

Therefore, we rewrite Equation (3) as follows,

$$\begin{aligned} \boldsymbol{E}_{i,j} &= Encrypt(h, \boldsymbol{T}, Id_i, \boldsymbol{c}_{i,j}) \\ &= (\boldsymbol{E}_{\boldsymbol{c},\boldsymbol{T}}, \boldsymbol{D}_{i,j}). \end{aligned} \tag{8}$$

- **Sign** (sk, Id_i, $\boldsymbol{c}$). Suppose a full-domain hash function $H : \{0,1\}^* \mapsto \mathbb{F}_p$ as a random oracle. The signature of source c is given by

$$\Delta = \zeta^{\sum_{i=1}^{t+n} c_i sk_i + \left(\sum_{i=1}^{t} c_i\right) H(Id_i) sk_{t+n+1}}, \tag{9}$$

where sk is the signature key such that $sk = \{sk_1, \ldots, sk_{t+n+1}\}, sk_i \xleftarrow{R} \mathbb{F}_p$. Then, the data blocks $\{c_i\}_{i-1}^{\sigma}$ and $\{\Delta_i\}_{i-1}^{\sigma}$ of the i-th generation are combined as follows:

$$\Theta_i = \left(\sum_{i=1}^{\sigma} T_i c_i, \prod_{i=1}^{\sigma} \Delta^{T_i}, Id_i \right). \tag{10}$$

- **Verify** (pk, $\boldsymbol{c}$, Id_i, Δ). When the public key pk, a data block $\boldsymbol{c}$, a generation Id_i, and the signature Δ are given, the compared computation is given by

$$\eta_1 = e(\Delta, o) \tag{11}$$

and

$$\eta_2 = e(\zeta, \prod_{i=1}^{t+n} h_i^{c_i} \cdot \prod_{i=1}^{t} h_{t+n+1}^{H(Id_i)c_i}). \tag{12}$$

where o is the generator of $\mathbb{G}$, $pk = (\zeta, o, \mathbb{G}, \mathbb{G}_D, \boldsymbol{h})$, and $\mu \xleftarrow{R} \mathbb{G}\{1\}$. $\mathbb{G}$ and $\mathbb{G}_D$ are two multiplicative cyclic groups, which satisfy $e : \mathbb{G} \times \mathbb{G} \longmapsto \mathbb{G}_D$ in a bilinear map, and $\boldsymbol{h} := \left\{o^{sk_1}, \ldots, o^{sk_{t+n+1}}\right\}$. When $\eta_1 = \eta_2$, the verification is successful; otherwise, it fails.

- **Decrypt** (h, $\boldsymbol{T}$, Id_i $\boldsymbol{c}$). When the secret key k and the pseudo-random function f are given, the decryption matrix can be computed as follows:

$$\boldsymbol{DE}_{\boldsymbol{c},\boldsymbol{T}} = \begin{bmatrix} c_{e_{i,1}}^{-1} & & \\ & \ddots & \\ & & c_{e_{i,t}}^{1} \end{bmatrix} \tag{13}$$

4.2. The Correctness and Security Analysis of Our Privacy-Preserving Sheme

In this subsection, we provide the correctness analysis of our privacy-preserving scheme with two theorems and proofs.

Theorem 1. *Given an augmented data block $\boldsymbol{c} \in \prod_i$ including coding vector $\boldsymbol{p}$ and native message $\boldsymbol{D}$, $\boldsymbol{Decrypt}(\boldsymbol{T}, Id_i \boldsymbol{Encrypt}(h, \boldsymbol{T}, Id_i, \boldsymbol{c})) = \boldsymbol{c}$.*

Proof of Theorem 1. According to Equation (8), the encrypted augmented data block c_E is given as follows:

$$\begin{aligned} \boldsymbol{c}_E &= \boldsymbol{E}_{\boldsymbol{c},\boldsymbol{T}} \cdot (\boldsymbol{p}, \boldsymbol{D}) \\ &= (\boldsymbol{E}_{\boldsymbol{c},\boldsymbol{T}} \cdot p, \boldsymbol{E}_{\boldsymbol{c},\boldsymbol{T}} \cdot \boldsymbol{D}), \end{aligned} \tag{14}$$

Then, according to our scheme, the decryption matrix can be expressed as follows:

$$\begin{aligned} \boldsymbol{c}_D &= \boldsymbol{DE}_{\boldsymbol{c},\boldsymbol{T}} \cdot \boldsymbol{c}_E \\ &= \boldsymbol{DE}_{\boldsymbol{c},\boldsymbol{T}} \cdot (\boldsymbol{E}_{\boldsymbol{c},\boldsymbol{T}} \cdot \boldsymbol{p}, \boldsymbol{E}_{\boldsymbol{c},\boldsymbol{T}} \cdot \boldsymbol{D}) \\ &= \begin{bmatrix} c_e^{-1} & & \\ & \ddots & \\ & & c_e^{1} \end{bmatrix} \cdot \left(\begin{bmatrix} c_e & & \\ & \ddots & \\ & & c_e \end{bmatrix} \cdot \boldsymbol{p}, \begin{bmatrix} c_e & & \\ & \ddots & \\ & & c_e \end{bmatrix} \cdot \boldsymbol{D} \right) \\ &= (\boldsymbol{p}, \boldsymbol{D}) \\ &= \boldsymbol{c} \end{aligned} \tag{15}$$

Therefore, The proof is completed. □

Theorem 2. *For any generation Id_i and $\boldsymbol{c} \in \mathbb{F}_p^{t+n}$, **Verify** ($pk$, $\boldsymbol{c}$, Id_i, Δ) is successful.*

Proof of Theorem 2. According to Equations (9)–(12), we have

$$\begin{aligned} \eta_1 &= e(\Delta, o) \\ &= e(\zeta^{\sum_{i=1}^{t+n} c_i sk_i + \left(\sum_{i=1}^{t} c_i\right) H(Id_i) sk_{t+n+1}}, o) \\ &= e(\zeta, o)^{\sum_{i=1}^{t+n} c_i sk_i + \left(\sum_{i=1}^{t} c_i\right) H(Id_i) sk_{t+n+1}} \end{aligned} \tag{16}$$

and

$$\begin{aligned} \eta_2 &= e(\zeta, \prod_{i=1}^{t+n} h_i^{c_i} \cdot \prod_{i-1}^{t} h_{t+n+1}^{H(Id_i)c_i}) \\ &= e(\zeta, \prod_{i=1}^{t+n} o^{sk_i c_i} \cdot \prod_{i-1}^{t} o^{sk_{t+n+1} H(Id_i) c_i}) \\ &= e(\zeta, o^{\sum_{i=1}^{t+n} c_i sk + \sum_{i=1}^{t} c_i H(Id_i) sk_{t+n+1}}) \\ &= e(\zeta, o)^{\sum_{i=1}^{t+n} c_i sk_i + \left(\sum_{i=1}^{t} c_i\right) H(Id_i) sk_{t+n+1}} \end{aligned} \tag{17}$$

Therefore, $\eta_1 = \eta_2$ can be held for any generation Id_i and $\boldsymbol{c} \in \mathbb{F}_p^{t+n}$. □

The security of our privacy-preserving scheme relies on the hardness of the discrete logarithm over $\mathbb{G}$, where for any $x \in \mathbb{Z}_p^*$ and given (g, g^x), x cannot be computed in any polynomial algorithm [36].

4.3. The Optimization Cluster Formulation Scheme Based on Repeated Game Model

After considering the data privacy and the trustworthiness of IoT devices, an effective trust cluster formulation scheme (ETCFS) is designed based on the repeated game for preserving the network stability and conserving the power consumption due to packet re-transmission. Many studies in the literature have reported that the repeated game model can solve the balance problem between network performance and resource consumption.

4.3.1. Repeated Game Model

In this sub-subsection, we first present a repeated game model based on the trustworthiness to elect the trust route IoT devices. Then, the subgame-perfect Nash equilibrium is given. Furthermore, the repeated game model is formally defined as follows:

(a) Attackers $A_r = \{A_1, A_2, \ldots, A_r\}$ and defenders $D_r = \{D_1, D_2, \ldots, D_r\}$ are the cooperating parties in the repeated game, where $r \in \mathbb{N}_+$.

(b) Given the utility function U_A^r and U_D^r, and the loss discount δ, the average utility is $\lim_{r\to\infty} \sum_{j=1}^{r} \frac{U_A}{r}$ and $\lim_{r\to\infty} \sum_{j=1}^{r} \frac{U_D}{r}$, where r is number of iterations according to the lifetime of the network. Furthermore, the total payoff for both parties are respectively as follows:

$$U_A = U_A^1 + \delta U_A^2 + \delta^2 U_A^3 + \ldots + \delta^{r-1} U_A^r = \sum_{r=1}^{r} \delta^{r-1} U_A^r, \tag{18}$$

$$U_D = U_D^1 + \delta U_D^2 + \delta^2 U_D^3 + \ldots + \delta^{r-1} U_D^r = \sum_{r=1}^{r} \delta^{r-1} U_D^r, \tag{19}$$

where the weight of the current and future payoff is inconsistent, and the future payoff is generally less than the weight of the current payoff.

(c) The proposed repeated game model is finite due to the power of the entire network being predetermined. Therefore, the finite repeated game can be solved by the backward method, which basically converges to the sub-game equilibrium.

4.3.2. The Solution of Repeated Game Model for Optimizing Cluster Formulation

In the IoT, the various IoT devices including pads, phones, and monitors are members of the cluster (CM). The network controller hopes that the IoT devices with higher energy and trustworthiness become cluster heads (CH). Furthermore, the energy level E of IoT devices is divided into two subsets, that is, E_h and E_l based on the remaining energy, where E_h is the set of nodes having energy more than or equal to the threshold E_{th}, and E_l is lower than E_{th}. Each IoT device in the cluster can select CH or CM according to the two strategies $S = CH, CM$. In addition, the payoff of players can be found in Table 1.

Table 1. The different payoffs under different behaviors of players.

Strategy	To Be CH	To Be CM
Normal	$U_{i,j}(N, CH)$, $U'_{i,j}(N, CH)$	$U_{i,j}(N, CM)$, $U'_{i,j}(N, CM)$
Malicious	$U_{i,j}(M, CH)$, $U'_{i,j}(M, CH)$	$U_{i,j}(M, CM)$, $U'_{i,j}(M, CM)$

Meanwhile, the network controller is a defender, and other IoT devices may be normal or malicious, so the utility function U_A^r and U_D^r in the iteration r can be defined as follows:

(a) Suppose that all members of E_h and E_l IoT devices become CH with no CM, and the payoffs of defender and attacker are decreasing. At this time, the cluster is illegal. Therefore, the utility of defender and attacker in the iteration r can be expressed as

$$\begin{cases} U_{D,T}^r = \alpha T_h - 2\theta C_h \\ U_{A,T}^r = \alpha T_l, \end{cases} \tag{20}$$

where α and θ are the weights of the reward and penalty, $\alpha + \theta = 1$, $\alpha, \theta \in [0, 1]$. T_h and T_l are the trustworthiness of low-energy and high-energy IoT devices. Meanwhile, C_h and C_l are the communication costs of high-energy and low-energy IoT devices.

(b) Suppose that E_h and E_l IoT devices respectively become CH and CM; the payoff of the defender is the highest, and that of the attacker is the lowest. Therefore, the utility of the defender and attacker in the iteration r can be expressed as

$$\begin{cases} U_{D,T}^r = 2\alpha T_h - \theta C_h \\ U_{A,T}^r = \alpha T_l - 2\theta C_l, \end{cases} \tag{21}$$

(c) Suppose that E_l and E_h IoT devices respectively become CH and CM, and the payoffs of the attacker are the highest. However, the CH with E_l can also help the network controller formulate a legal cluster. Therefore, the weight of reward and penalty are predefined, and the utility of defender and attacker in the iteration r are given by

$$\begin{cases} U_{D,T}^r = T_h - \theta C_h \\ U_{A,T}^r = 2\alpha T_l - \theta C_l, \end{cases} \tag{22}$$

(d) Suppose that E_l and E_h IoT devices have become CM with no CH; then, the cluster is illicit. Therefore, the respective utilities of the defender and attacker in the iteration r are given by

$$\begin{cases} U_{D,T}^r = \alpha T_h - 2\theta C_h \\ U_{A,T}^r = \alpha T_l - \theta C_l, \end{cases} \tag{23}$$

Then, we achieve subgame-perfect Nash equilibrium $(\psi^*, \xi^*) = (1, 0)$ according to the evolutionarily stable strategy (ESS) [35]. The details can be seen in Appendix A.

5. Simulation Result and Discussion

This section shows the simulation result of the energy-efficient privacy-preserving scheme and ETCFS scheme in IoTs. We use the OMNET++ simulator to construct the network model with malicious activity and compute the trustworthiness of each IoT device. The details of parameters used to configure the network model are given in Table 2. Then, we compare the ETCFS scheme with state-of-the-art TDDG [33], HIDS [37], and LHIDS [38] to show the effectiveness of the above schemes. In addition, the maximum running iteration of the simulation is 100.

Table 2. The simulation network parameters.

Parameter	Value	Parameter	Value
Network region	200×200 m^2	Communication radius	2 m
Number of IoT devices	100	Sensing radius	1 m
Initial trustworthiness	0.6	Attack intensity	0.2–0.6
Packet length	400–1000	α, θ, δ	0.2, 0.2, 0.4
Initial energy	10 J	Maximum iteration	100
Eth	4 J	Hop limit	2

5.1. Simulation Parameter Setting

In this subsection, we define the metrics, including trustworthiness, the running time of the privacy-preserving scheme, and the lifetime of the IoT, to discuss the performance of the privacy-preserving scheme and ETCFS scheme.

(a) The trustworthiness of each IoT device consists of direct trust T_{direct} and indirect trust $T_{indirect}$. The total trust is defined as follows:

$$T_{total} = \lambda_1 T_{direct} + \lambda_2 T_{indirect} \tag{24}$$

where λ_1 and λ_2 are the weight parameters of direct and indirect trust, which satisfy $\lambda_1 + \lambda_2 = 1$. The trust evaluation method including direct and indirect trust can be found in [39].

(b) The running time of the privacy-preserving scheme reflects the effectiveness of our scheme, which can run faster than previous schemes [40,41], while satisfying the demand for data privacy.

(c) The lifetime of the IoT reflects lower resource consumption than in other literature. Furthermore, the lifetime of IoTs with our repeated game model is the highest.

5.2. Performance Comparison

In this subsection, we compare the performance of the proposed privacy-preserving and ETCFS scheme with the state-of-the-art methods under the preset network parameters.

(a) Energy Efficiency with T-S Fuzzy Trust Model: In Figures 2 and 3, the energy consumption of our T-S fuzzy trust model is compared with NCS0-, NCS1-, and ID-based schemes. The result of the simulation shows that our scheme has the lowest energy consumption. As the number of attack nodes in the IoT increases, the energy required for trust evaluation gradually increases. However, the energy consumption of our scheme has been in a stable state, and there is no significant increase. Meanwhile, our scheme has the highest remaining energy than other schemes when the $iteration = [30–100]$.

(b) Time Efficiency of Our Privacy-Preserving Scheme: In Figure 4, the runtime of our trust-based privacy-preserving scheme is the lowest compared to the other three methods. In addition, our scheme has higher stability according to the magnitude of running time variation.

(c) Time Consumption with Cluster Formulation: In Figures 5 and 6, we compare the time consumption when the hop limit is 1 and 2 under camouflage attack. Based on theo-

retically verifying that the proposed repeated game has effective game equilibrium, we also find our game-based cluster formulation has the lowest time consumption.

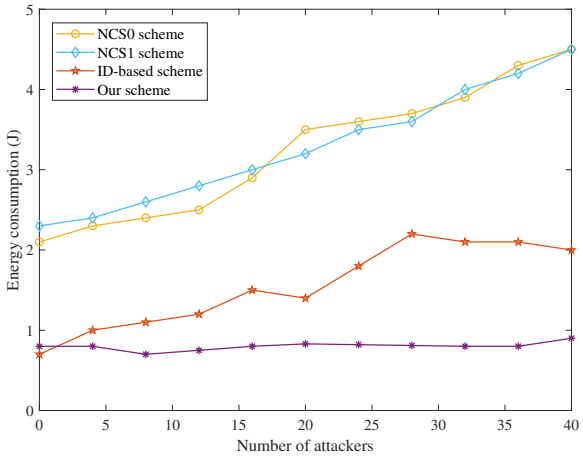

Figure 2. The energy consumption with T-S fuzzy trust model.

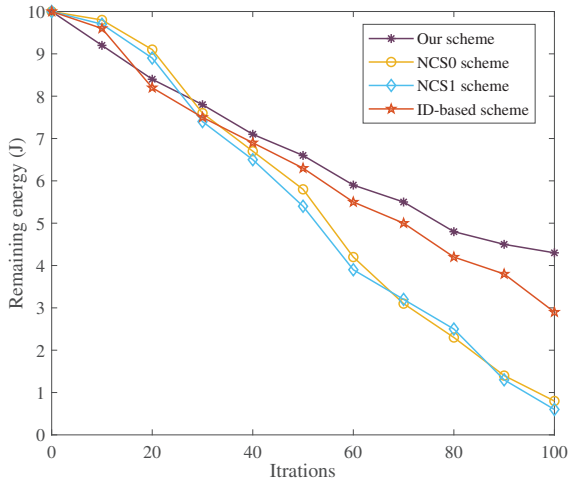

Figure 3. The remaining energy for the T-S fuzzy trust model with different iterations.

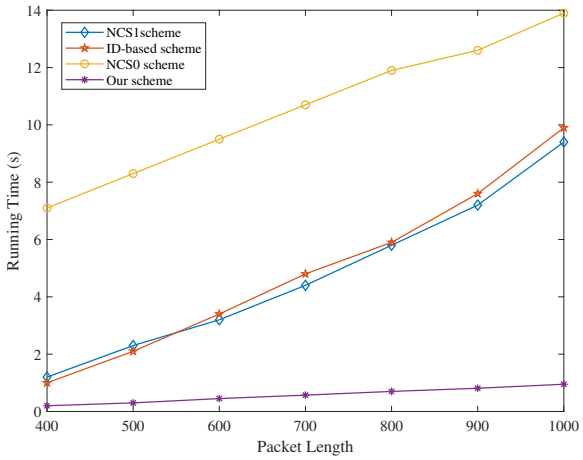

Figure 4. The running time of signature, encryption, and verification in different schemes against packet length.

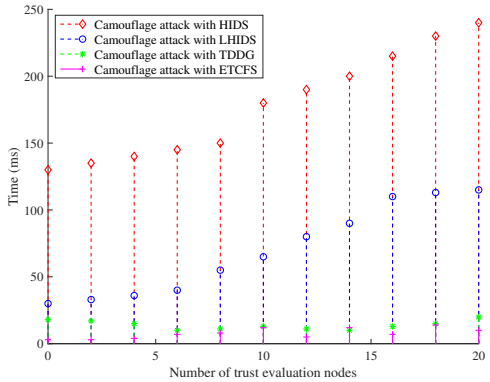

Figure 5. The time consumption with cluster formulation under different schemes in camouflage attack (hop limit = 1).

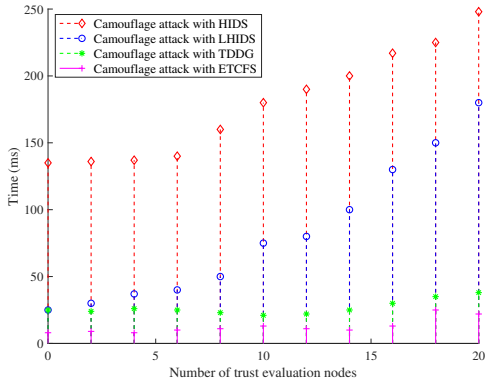

Figure 6. The time consumption with cluster formulation under different schemes in camouflage attack (hop limit = 2).

6. Conclusions

This paper investigates a novel fuzzy-based privacy-preserving scheme to defend against pollution attacks in coding IoTs and constructs a repeated game model to balance data security and energy consumption. We propose a T-S fuzzy trust evaluation method to replace the traditional cryptography scheme and reduce the energy consumption in IoTs. Then, we introduce the trust-based privacy-preserving scheme, in which the security relies on the hardness of the discrete logarithm. Finally, an optimal cluster formulation based on the repeated game model is proposed to balance the data security and energy consumption. The result shows that the cluster formulation can mitigate the camouflage attack. In addition, our scheme only considers two types of attacks in IoTs. Therefore, we will consider more kinds of attacks on IoT data, and construct more effective privacy-preserving schemes in future work.

Author Contributions: Conceptualization, L.C. and M.Z.; methodology, L.C.; software, M.Z.; validation, L.C. and M.Z.; formal analysis, M.Z.; investigation, L.C.; resources, M.Z.; data curation, L.C.; writing—original draft preparation, M.Z.; writing—review and editing, L.C.; visualization, M.Z.; supervision, L.C.; project administration, M.Z.; funding acquisition, L.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Nature Science Foundation of China under (grant no. 61562059, 61461027, 61462060).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Appendix A.1. The Optimizing Solution of Defenders

$$\begin{aligned} U_D^{E_h\to \mathrm{CH}} &= \sum_{r=1}^{r} \delta^{r-1}[\xi(\alpha T_h - 2\theta C_h) + (1-\xi)(2\alpha T_h - \theta C_h)] \\ U_D^{E_h\to \mathrm{CM}} &= \sum_{r=1}^{r} \delta^{r-1}[\xi(T_h - \theta C_h) + (1-\xi)(\alpha T_h - 2\theta C_h)] \\ U_D^{E_l\to \mathrm{CH}} &= \sum_{r=1}^{r} \delta^{r-1}[\xi(\alpha T_h - 2\theta C_h) + (1-\xi)(T_h - \theta C_h)] \\ U_D^{E_l\to \mathrm{CM}} &= \sum_{r=1}^{r} \delta^{r-1}[\xi(2\alpha T_h - \theta C_h) + (1-\xi)(\alpha T_h - 2\theta C_h)], \end{aligned} \tag{A1}$$

$$\begin{aligned} \overline{U_D} &= \psi U_D^{E_h\to \mathrm{CH}} + (1-\psi)U_D^{E_h\to \mathrm{CM}} + (1-\psi)U_D^{E_l\to \mathrm{CH}} + \psi U_D^{E_l\to \mathrm{CM}} \\ &= \sum_{r=1}^{r} \delta^{r-1} \begin{bmatrix} \psi\xi(\alpha T_h - 2\theta C_h) + \psi(1-\xi)(2\alpha T_h - \theta C_h) \\ +(1-\psi)\xi(T_h - \theta C_h) + (1-\psi)(1-\xi)(\alpha T_h - 2\theta C_h) \\ +(1-\psi)\xi(\alpha T_h - 2\theta C_h) + (1-\psi)(1-\xi)(T_h - \theta C_h) \\ +\psi\xi(2\alpha T_h - \theta C_h) + \psi(1-\xi)(\alpha T_h - 2\theta C_h) \end{bmatrix} \\ &= \sum_{r=1}^{r} \delta^{r-1}[(\alpha T_h - 2\theta C_h) + (2\alpha T_h - \theta C_h)\psi + (T_h - \theta C_h)(1-\psi)] \\ &= \sum_{r=1}^{r} \delta^{r-1}[(1+2\psi)\alpha T_h - 3\theta C_h + T_h(1-\psi)] \end{aligned} \tag{A2}$$

$$\begin{aligned} \frac{d\psi}{dr} &= \psi(U_D^{E_h\to \mathrm{CH}} + U_D^{E_l\to \mathrm{CM}} - \overline{U_D}) \\ &= \psi \sum_{r=1}^{r} \delta^{r-1} \begin{bmatrix} \xi(\alpha T_h - 2\theta C_h) + (1-\xi)(2\alpha T_h - \theta C_h) \\ +\xi(2\alpha T_h - \theta C_h) + (1-\xi)(\alpha T_h - 2\theta C_h) \\ -[(1+2\psi)\alpha T_h - 3\theta C_h + T_h(1-\psi)] \end{bmatrix} \\ &= \psi \sum_{r=1}^{r} \delta^{r-1}[(2-2\psi)\alpha T_h - (1-\psi)T_h)] \\ &= \sum_{r=1}^{r} \delta^{r-1}\psi(1-\psi)(2\alpha T_h - T_h) \end{aligned} \tag{A3}$$

when $\frac{d\psi}{dr} = 0$, the player D achieves a stable state. Therefore, when $\psi* = 0$ or 1, the player D has the highest payoff.

Appendix A.2. The Optimizing Solution of Attackers

Similarly, the expression of player A is obtained as follows:

$$\begin{aligned} U_A^{E_h\to \mathrm{CH}} &= \sum_{r=1}^{r} \delta^{r-1}[\psi(\alpha T_l) + (1-\psi)(\alpha T_l - 2\theta C_l)] \\ U_A^{E_h\to \mathrm{CM}} &= \sum_{r=1}^{r} \delta^{r-1}[\psi(2\alpha T_l - \theta C_l) + (1-\psi)(\alpha T_l - \theta C_l)] \\ U_A^{E_l\to \mathrm{CH}} &= \sum_{r=1}^{r} \delta^{r-1}[\psi(\alpha T_l) + (1-\psi)(2\alpha T_l - \theta C_l)] \\ U_A^{E_l\to \mathrm{CM}} &= \sum_{r=1}^{r} \delta^{r-1}[\psi(\alpha T_l - 2\theta C_l) + (1-\psi)(\alpha T_l - \theta C_l)] \end{aligned} \tag{A4}$$

$$\begin{aligned}\overline{U_A} &= \xi U_A^{E_h\to \mathrm{CH}} + (1-\xi)U_A^{E_h\to \mathrm{CM}} + (1-\xi)U_A^{E_l\to \mathrm{CH}} + \xi U_A^{E_l\to \mathrm{CM}} \\ &= \sum_{r=1}^{r} \delta^{r-1}\left[\begin{array}{c} \xi(\alpha T_l - 2\theta C_l) + (1-\xi)(2\alpha T_l - \theta C_l) \\ +(1-\psi)(\alpha T_l - \theta C_l) + \psi(\alpha T_l) \end{array}\right] \\ &= \sum_{r=1}^{r} \delta^{r-1}[(3-\xi)\alpha T_l + (\psi - \xi - 2)\theta C_l]\end{aligned} \tag{A5}$$

$$\begin{aligned}\frac{d\xi}{dr} &= \sum_{r=1}^{r} \delta^{r-1}\xi(U_A^{E_h\to \mathrm{CM}} + U_A^{E_l\to \mathrm{CH}} - \overline{U_A}) \\ &= \sum_{r=1}^{r} \delta^{r-1}\xi\left[\begin{array}{c} \psi(2\alpha T_l - \theta C_l) + (1-\psi)(\alpha T_l - \theta C_l) + \psi(\alpha T_l) \\ +(1-\psi)(2\alpha T_l - \theta C_l) - (3-\xi)\alpha T_l - (\psi - \xi - 2)\theta C_l \end{array}\right] \\ &= \sum_{r=1}^{r} \delta^{r-1}\xi[(\psi + \xi)\alpha T_l + \xi\theta C_l]\end{aligned} \tag{A6}$$

When the $\psi^* = 0$; the $\xi^* = 0$, relatively; the $\psi^* = 1$; the $\xi^* = 0$; and the optimizing payoffs of defender and attacker can be achieved. Furthermore, according to the reality, the subgame-perfect nash equilibrium is obtained as $(\psi^*, \xi^*) = (1, 0)$.

References

1. Noor, M.B.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2018**, *148*, 283–294. [CrossRef]
2. Rani, R.; Kumar, S.; Dohare, U. Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach. *IEEE Internet Things J.* **2019**, *6*, 8421–8432. [CrossRef]
3. Wu, Y.; Kang, B.; Wu, H. Strategies of attack–defense game for wireless sensor networks considering the effect of confidence level in fuzzy environment. *Eng. Appl. Artif. Intell.* **2021**, *102*, 104238. [CrossRef]
4. Hou, J.; Qiao, J.; Han, X. Energy-Saving Clustering Routing Protocol for Wireless Sensor Networks Using Fuzzy Inference. *IEEE Sens. J.* **2022**, *22*, 2845–2857. [CrossRef]
5. Kumar, S.; Goswami, A.; Gupta, R.; Singh, S.P.; Lay-Ekuakille, A. A Game-Theoretic Approach for Cost-Effective Multicast Routing in the Internet of Things. *IEEE Internet Things J.* **2022**. [CrossRef]
6. Adil, M.; Khan, R.; Almaiah, M.A.; Binsawad, M.; Ali, J.; Saaidah, A.A.; Ta, Q.T.H. An Efficient Load Balancing Scheme of Energy Gauge Nodes to Maximize the Lifespan of Constraint Oriented Networks. *IEEE Access* **2020**, *8*, 148510–148527. [CrossRef]
7. Zhang, P.; Wang, Y.; Kumar, N.; Jiang, C.; Shi, G. A Security and Privacy-Preserving Approach Based on Data Disturbance for Collaborative Edge Computing in Social IoT Systems. *IEEE Trans. Comput. Soc. Syst.* **2021**, *9*, 97–108. [CrossRef]
8. Zhao, F.; Kalker, T.; Medard, M.; Han, K.J. Signatures for Content Distribution with Network Coding. In Proceedings of the 2006 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 22–24 March 2006.
9. Peng, Z.; Jiang, Y.; Lin, C.; Yao, H.; Shen, X. Padding for orthogonality: Efficient subspace authentication for network coding. In Proceedings of the Infocom, Shanghai, China, 10–15 April 2011.
10. Guangjun, L.; Bin, W. Secure network coding against intra/inter-generation pollution attacks. *China Commun.* **2013**, *10*, 100–110. [CrossRef]
11. Li, Y.; Yao, H.; Chen, M.; Jaggi, S.; Rosen, A. RIPPLE Authentication for Network Coding. In Proceedings of the 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9. [CrossRef]
12. Cheng, C.; Jiang, T. An Efficient Homomorphic MAC with Small Key Size for Authentication in Network Coding. *IEEE Trans. Comput.* **2013**, *62*, 2096–2100. [CrossRef]
13. Cheng, C.; Lee, J.; Jiang, T.; Takagi, T. Security Analysis and Improvements on Two Homomorphic Authentication Schemes for Network Coding. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 993–1002. [CrossRef]
14. Li, T.; Chen, W.; Tang, Y.; Yan, H. A Homomorphic Network Coding Signature Scheme for Multiple Sources and its Application in IoT. *Secur. Commun. Netw.* **2018**, *2018*, 9641273. [CrossRef]
15. Fiandrotti, A.; Gaeta, R.; Grangetto, M. Simple Countermeasures to Mitigate the Effect of Pollution Attack in Network Coding-Based Peer-to-Peer Live Streaming. *IEEE Trans. Multimed.* **2015**, *17*, 562–573. [CrossRef]
16. Antonopoulos, A.; Verikoukis, C. COPS: Cooperative Statistical Misbehavior Mitigation in Network-Coding-aided Wireless Networks. *IEEE Trans. Ind. Inform.* **2017**, *14*, 1436–1446. [CrossRef]
17. Lawrence, T.; Li, F.; Ali, I.; Kpiebaareh, M.Y.; Christopher, T. An HMAC-based authentication scheme for network coding with support for error correction and rogue node identification. *J. Syst. Archit.* **2021**, *116*, 102051. [CrossRef]
18. Sodhro, A.H.; Sennersten, C.; Ahmad, A. Towards Cognitive Authentication for Smart Healthcare Applications. *Sensors* **2022**, *22*, 2101. [CrossRef]
19. Li, X.J.; Yan, J.J.; Yang, G.H. Adaptive Fault Estimation for T-S Fuzzy Interconnected Systems Based on Persistent Excitation Condition via Reference Signals. *IEEE Trans. Cybern.* **2018**, *49*, 2822–2834. [CrossRef]

20. Rajeswari, A.R.; Kulothungan, K.; Ganapathy, S.; Kannan, A. Trusted energy aware cluster based routing using fuzzy logic for WSN in IoT. *J. Intell. Fuzzy Syst.* **2021**, *40*, 9197–9211. [CrossRef]
21. Cao, K.-R.; Liu, J.-Q.; Huang, X.-L.; Gao, X.-Z.; Ban, X.-J. Stability Analysis of T–S Fuzzy Control Systems by Using Set Theory. *J. Harbin Inst. Technol.* **2012**, *19*, 7–11.
22. Han, J.; Zhang, H.; Wang, Y.; Zhang, K. Fault Estimation and Fault-Tolerant Control for Switched Fuzzy Stochastic Systems. *IEEE Trans. Fuzzy Syst.* **2018**, *26*, 2993–3003. [CrossRef]
23. Dong, J.; Wu, Y.; Yang, G.H. A New Sensor Fault Isolation Method for T–S Fuzzy Systems. *IEEE Trans. Cybern.* **2017**, *47*, 2437–2447. [CrossRef]
24. Liu, M.; Cao, X.; Shi, P. Fuzzy-model-based fault-tolerant design for nonlinear stochastic systems against simultaneous sensor and actuator faults. *IEEE Trans. Fuzzy Syst.* **2012**, *21*, 789–799. [CrossRef]
25. Liu, J.; Wei, L.; Xie, X.; Tian, E.; Fei, S. Quantized Stabilization for T–S Fuzzy Systems With Hybrid-Triggered Mechanism and Stochastic Cyber-Attacks. *IEEE Trans. Fuzzy Syst.* **2018**, *26*, 3820–3834. [CrossRef]
26. Zhang, Z.; Niu, Y.; Song, J. Input-to-State Stabilization of Interval Type-2 Fuzzy Systems Subject to Cyberattacks: An Observer-Based Adaptive Sliding Mode Approach. *IEEE Trans. Fuzzy Syst.* **2019**, *28*, 190–203. [CrossRef]
27. Yan, J.J.; Yang, G.H.; Li, X.J. Fault detection in finite frequency domain for T-S fuzzy systems with partly unmeasurable premise variables. *Fuzzy Sets Syst.* **2020**, *421*, 158–177. [CrossRef]
28. Mohamed, A.; Karim, S.; Maha, E.; Osamu, M.; Hiroshi, F.; Adel, A.R. Game Theory Meets Wireless Sensor Networks Security Requirements and Threats Mitigation: A Survey. *Sensors* **2016**, *16*, 1003.
29. Riahi Sfar, A.; Challal, Y.; Moyal, P.; Natalizio, E. A Game Theoretic Approach for Privacy Preserving Model in IoT-Based Transportation. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 4405–4414. [CrossRef]
30. Abdalzaher, M.S.; Seddik, K.; Muta, O.; Mohamed. Using Stackelberg game to enhance cognitive radio sensor networks security. *IET Commun.* **2017**, *11*, 1503–1511. [CrossRef]
31. Abdalzaher, M.S.; Seddik, K.; Muta, O. An effective Stackelberg game for high-assurance of data trustworthiness in WSNs. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017.
32. Abdalzaher, M.S.; Seddik, K.; Muta, O. Using repeated game for maximizing high priority data trustworthiness in Wireless Sensor Networks. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017.
33. Duan, J.; Gao, D.; Yang, D.; Foh, C.H.; Chen, H.H. An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications. *Internet Things J.* **2014**, *1*, 58–69. [CrossRef]
34. Li, Y.; Shi, L.; Chen, T. Detection against linear deception attacks on multi-sensor remote state estimation. *IEEE Trans. Control. Netw. Syst.* **2017**, *5*, 846–856. [CrossRef]
35. Yan, S.; Peng, M.; Cao, X. A Game Theory Approach for Joint Access Selection and Resource Allocation in UAV Assisted IoT Communication Networks. *IEEE Internet Things J.* **2019**, *6*, 1663–1674. [CrossRef]
36. Liu, X.; Huang, J.; Wu, Y.; Zong, G. A privacy-preserving signature scheme for network coding. *IEEE Access* **2019**, *7*, 109739–109750. [CrossRef]
37. Yan, K.; Wang, S.; Wang, S.; Liu, C. Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network. In Proceedings of the 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, China, 9–11 July 2010; Volume 1, pp. 114–118.
38. Sedjelmaci, H.; Senouci, S.M.; Taleb, T. An accurate security game for low-resource IoT devices. *IEEE Trans. Veh. Technol.* **2017**, *66*, 9381–9393. [CrossRef]
39. Qi, C.; Huang, J.; Wang, B.; Wang, H. A Novel Privacy-Preserving Mobile-Coverage Scheme Based on Trustworthiness in HWSNs. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9935780. [CrossRef]
40. Boneh, D.; Freeman, D.; Katz, J.; Waters, B. Signing a linear subspace: Signature schemes for network coding. In Proceedings of the International Workshop on Public Key Cryptography, Irvine, CA, USA, 18–20 March 2009; pp. 68–87.
41. Lin, Q.; Yan, H.; Huang, Z.; Chen, W.; Shen, J.; Tang, Y. An ID-based linearly homomorphic signature scheme and its application in blockchain. *IEEE Access* **2018**, *6*, 20632–20640. [CrossRef]