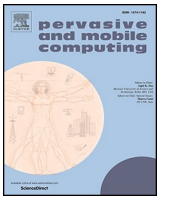
Pervasive and Mobile Computing 105 (2024) 101995

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc



An energy-aware secure routing scheme in internet of things networks via two-way trust evaluation

Tingxuan Fu [a,*], Sijia Hao [a], Qiming Chen [a], Zihan Yan [a], Huawei Liu [a], Amin Rezaeipanah [b,*]

[a] Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming, Yunnan, 650504, China
[b] Department of Computer Engineering, University of Rahjuyan Danesh Borazjan, Bushehr, Iran

ARTICLE INFO

Keywords:
Internet of Things
Energy-aware
Security
Two-way trust
Generative flow networks
Routing scheme

ABSTRACT

The rapid advancement of technology has led to the proliferation of devices connected to the Internet of Things (IoT) networks, bringing forth challenges in both energy management and secure data communication. In addition to energy constraints, IoT networks face threats from malicious nodes, which jeopardize the security of communications. To address these challenges, we propose an Energy-aware secure Routing scheme via Two-Way Trust evaluation (ERTWT) for IoT networks. This scheme enhances network protection against various attacks by calculating trust values based on energy trust, direct trust, and indirect trust. The scheme aims to enhance the efficiency of data transmission by dynamically selecting routes based on both energy availability and trustworthiness metrics of fog nodes. Since trust management can guarantee privacy and security, ERTWT allows the service requester and the service provider to check each other's safety and reliability at the same time. In addition, we implement Generative Flow Networks (GFlowNets) to predict the energy levels available in nodes in order to use them optimally. The proposed scheme has been compared with several advanced energy-aware and trust-based routing protocols. Evaluation results show that ERTWT more effectively detects malicious nodes while achieving better energy efficiency and data transmission rates.

1. Introduction

The Internet of Things (IoT) is a vast network of interconnected devices that communicate and exchange data without human intervention [1]. IoT architecture is typically composed of three layers: the perception layer, responsible for data collection from sensors; the network layer, which transmits data; and the application layer, where data is processed and used for various services [2,3]. With the exponential growth in the number of IoT devices, the volume of generated data has surged drastically. Traditional cloud data centers, while effective for centralized processing, are often overwhelmed by the sheer amount of data produced [4]. These centers struggle to process and store data efficiently due to latency and bandwidth limitations, especially for real-time applications. To address these limitations, fog computing has emerged as an extension of cloud computing, bringing computational resources closer to the edge of the network [5–7]. The goal of fog computing in IoT architecture is to improve service delivery by reducing latency and enhancing data processing capabilities near end-users. In fog computing, fog nodes (also known as fog servers) act as service providers,

* Corresponding authors.
E-mail addresses: daqingftx@163.com (T. Fu), 202210417115@stu.kust.edu.cn (S. Hao), 202210405308@stu.kust.edu.cn (Q. Chen), 202210405130@stu.kust.edu.cn (Z. Yan), liuhuawei@stu.kust.edu.cn (H. Liu), amin.rezaeipanah@gmail.com (A. Rezaeipanah).

https://doi.org/10.1016/j.pmcj.2024.101995
Received 19 July 2024; Received in revised form 22 September 2024; Accepted 14 October 2024
Available online 16 October 2024

performing tasks such as data storage, processing, and computational offloading. On the other hand, fog clients, which include IoT devices and sensors, request services from these fog nodes [2]. A fog client refers to any IoT device or sensor that communicates with fog nodes for data processing, storage, or computational tasks [8,9]. This paradigm shift not only improves service efficiency but also enables faster responses for time-sensitive IoT applications.

However, fog computing introduces its own set of challenges, particularly in terms of energy efficiency and security [10]. Fog nodes are often deployed in resource-constrained environments where energy consumption must be minimized. Moreover, the distributed nature of fog computing exposes it to various security threats. Unlike cloud environments, where centralized security mechanisms are more robust, fog nodes and clients are more vulnerable to attacks, especially those related to routing and data transmission [11,12]. Typically, sensor nodes are deployed in hostile environments, making them susceptible to various forms of attacks, particularly routing attacks. Traditional cryptographic techniques, malicious node detection algorithms, and secure routing protocols, while effective in certain contexts, require substantial computational power, leading to high energy consumption [13]. This makes them unsuitable for IoT environments where energy conservation is critical. To counter internal attacks initiated by compromised sensor nodes, trust-based security mechanisms are more efficient. At the same time, the efficient use of energy remains a crucial factor that significantly impacts the overall performance of IoT networks [2,14].

In this regard, trust management systems in fog computing play a vital role in addressing these security concerns [15,16]. The purpose of such systems is to evaluate the trustworthiness of devices and nodes within the network, ensuring secure data transmission [17]. Trust can be categorized into direct trust, which is derived from the direct interactions between nodes, and indirect trust, which is based on recommendations or observations from other nodes. In these systems, two key entities are considered: the trustor (the entity evaluating trust) and the trustee (the entity being evaluated) [18,19]. Proper trust evaluation ensures that only trustworthy nodes are involved in critical communication processes, enhancing both security and energy efficiency [20].

Existing works in IoT routing protocols often face limitations in balancing energy efficiency and security. Many traditional security mechanisms, such as cryptographic methods and malicious node detection algorithms, are computationally intensive, leading to excessive energy consumption. This makes them impractical for energy-constrained IoT environments [21]. Additionally, these approaches typically rely on centralized cloud-based architectures, which can introduce high latency and bandwidth issues, especially as the number of IoT devices continues to grow [1,3]. Moreover, current trust management systems in fog computing are either too simplistic or fail to adequately account for both direct and indirect trust, leaving networks vulnerable to internal attacks from compromised nodes. The motivation behind incorporating mutual trust lies in the ability to mitigate risks posed by malicious entities while optimizing the performance of resource-constrained IoT networks [22,23]. These challenges have motivated the design of trust management systems based on two-way trust evaluation combined with energy-aware routing, which has gained significant attention from researchers in recent years [24–26]. By addressing both security and energy efficiency, these systems aim to overcome the limitations of traditional methods, providing more robust solutions for IoT networks that are increasingly exposed to security threats and energy constraints. This ensures not only secure data transmission but also optimal energy usage, enabling IoT networks to remain efficient and protected against evolving security threats [27].

In this work, we propose an Energy-aware secure Routing scheme via Two-Way Trust evaluation (ERTWT) to address the challenges of energy efficiency and security in IoT networks. By utilizing energy trust, direct trust, and indirect trust, ERTWT dynamically selects the most efficient and secure routes based on trustworthiness and energy availability. Furthermore, the implementation of Generative Flow Networks (GFlowNets) allows for the prediction of energy levels in nodes, optimizing their use while ensuring secure communication. Through the two-way trust evaluation, both the service requester and provider can assess each other's reliability, ensuring secure data exchange and reducing the risk of malicious attacks. Our proposed scheme has demonstrated superior performance in comparison to existing energy-aware and trust-based routing protocols, particularly in its ability to detect malicious nodes while maintaining energy efficiency.

The main contributions of this paper are as follows:

- We introduce an energy-efficient routing algorithm that dynamically selects routes in IoT networks based on the energy availability of nodes, optimizing resource usage and extending the network's lifespan.
- The proposed system incorporates a novel two-way trust evaluation mechanism that allows both service requesters and service providers (fog nodes and clients) to assess each other's trustworthiness, ensuring secure communication in IoT environments.
- We implement GFlowNets to predict energy levels in fog nodes, enhancing the optimal utilization of energy resources in the network.

The remainder of the paper is organized as follows: Section 2 reviews the related work. Section 3 describes the system model. Section 4 presents the proposed scheme. Section 5 demonstrates the experimental results. Finally, Section 6 concludes the paper.

2. Related works

In recent years, a variety of trust-based and energy-aware routing protocols have been proposed to enhance security and energy efficiency in IoT and fog computing environments [28–30]. Trust-based schemes such as ESFRM (Efficient and Secure Fog-Based Routing Mechanism) [31] and MTTM (Multi-Trust Metric Model) [32] focus on calculating trust scores to ensure secure routing by identifying malicious or unreliable nodes. These protocols typically rely on direct and indirect trust evaluations to detect misbehaving nodes, ensuring that data is routed through trustworthy paths [33]. However, they often face limitations in dynamic environments were node mobility or behavior changes rapidly, leading to slow convergence or inaccurate trust assessments. Moreover, many

trust-based schemes assume static network topologies, which reduces their effectiveness in highly dynamic settings like IoT, where nodes frequently move and interact with new devices [34]. On the other hand, energy-aware routing protocols such as EASR (Energy Aware and Secure Routing) [35] emphasize energy optimization by selecting routes that minimize energy consumption during data transmission. These protocols often employ clustering or hierarchical routing mechanisms to reduce the communication overhead and prolong the network's lifetime. While effective in reducing energy usage, most energy-aware models do not fully integrate trust mechanisms, potentially leaving the network vulnerable to attacks [36,37]. Furthermore, these protocols may struggle in environments where energy-efficient and secure routing must be balanced, as energy conservation can conflict with the need for secure, trust-based routing paths [38,39].

Wang et al. [40] present a two-way Trust Management System (TMS) for fog computing, aimed at improving the security and reliability of interactions between service requesters and providers. While this model is effective in dynamically calculating trust scores using direct observations and recommendations, it faces challenges in highly dynamic environments. The reliance on indirect recommendations can lead to delayed trust updates, reducing the system's responsiveness to malicious behaviors. Additionally, the use of social relationships as a criterion may not always be applicable in larger, more heterogeneous networks, limiting its scalability. Meanwhile, Bakhtiari et al. [41] propose the GALA trust model, which combines Genetic Algorithms (GA) and Learning Automaton (LA) to optimize trust management in fog environments. Although the hybrid approach enhances the exploration of the search space for optimal trust solutions, its reliance on GA and LA increases computational complexity, potentially leading to higher resource consumption in fog nodes. This is a critical limitation in resource-constrained environments where computational efficiency is vital. Moreover, the model's performance is heavily influenced by the crossover rate, making it sensitive to parameter tuning, which could limit its adaptability across various network settings.

Rehman et al. [42] introduce a lightweight trust management mechanism named FogTrust, which employs a multi-layer architecture involving edge nodes, a trusted agent, and the fog layer. This design facilitates secure communication between IoT nodes and the fog layer, reducing the burden on individual nodes while ensuring data integrity through encrypted trust values. However, the reliance on a centralized trust agent may introduce a single point of failure, potentially compromising the system's resilience against attacks. Additionally, while the aggregation of trust values by the agent aims to enhance accuracy, it may also result in delays in trust updates, which can hinder the timely detection of malicious nodes. The model's performance could also be impacted in highly dynamic environments where node mobility or behavior changes rapidly, as the system may struggle to adapt quickly to new trust dynamics. Zheng et al. [43] present a reliable distributed trust management model named TFog, designed to secure interactions among industrial IoT fog nodes. The model features clearly defined components and collaborative methods that enable independent operation on fog nodes in a scalable manner. It introduces innovative recommendation filtering algorithms, bi-directional interaction ratings, and multi-party trust update strategies to effectively counteract trust attacks.

Yadav and Baranwal [44] propose a responsibility-based trust revision model known as ReTREM, designed to evaluate and monitor the trustworthiness of fog nodes by categorizing them based on their responses to service quality violations. This model incorporates distinct penalty mechanisms aimed at deterring malicious behaviors while using two types of trust scores—one based on reliability metrics and feedback ratings (TS1) and the other provided by a fog broker (TS2). However, the model's reliance on subjective assessments of service quality can introduce biases, particularly if feedback mechanisms are manipulated by malicious nodes. Additionally, the complexity of implementing multiple penalty and reward mechanisms may result in increased computational overhead, potentially straining resources in a fog computing environment. Furthermore, ReTREM's effectiveness in dynamic contexts may be limited, as rapid changes in node behavior or service quality could lead to delayed or inaccurate trust assessments. Consequently, the gap in existing literature highlights the need for hybrid models that can simultaneously address security and energy efficiency while adapting to the dynamic and heterogeneous nature of fog and IoT networks.

Zero-trust routing schemes focus on enhancing security by eliminating the assumption of trust within network interactions, requiring all entities to verify their identities and continuously assess trustworthiness, regardless of their location within the network [45,46]. These schemes advocate for strict authentication and authorization processes for all communications, ensuring that even trusted devices are subjected to scrutiny [47]. By employing principles such as least privilege and micro-segmentation, zero-trust models mitigate risks associated with compromised nodes and unauthorized access, thereby improving the overall resilience of routing protocols in dynamic environments like fog computing. However, the implementation of zero-trust frameworks often involves increased complexity and resource demands, as constant monitoring and verification can lead to higher latency and overhead [48,49]. Additionally, the reliance on robust identity management systems can present challenges in scalability, especially in large networks with numerous interconnected devices. As an example of zero-trust routing, Ali et al. [50] introduced a trust-aware authentication scheme in Zero-Trust Security (ZTS). Task offloading is executed using the State-Action-Reward-State-Action (SARSA) [51] algorithm. This ensures legitimate user identification while addressing edge server resource constraints to minimize overall task completion time.

3. System model

The aim of trust management systems in fog environment is to identify and prevent malicious fog nodes and bad fog clients [52,53]. A malicious fog node behaves like a legitimate node but has been compromised by attackers or replaced with a counterfeit node. A malicious node with a high trust score can potentially deceive any server into accepting it. To predict future trust and avoid uncertainty, trust management systems must gather object-related information from observations and direct recommendations [54,55]. Trust management involves two entities: the trustor and trustee. The sequence of interactions between a fog client and fog node aims to establish a reliable connection. A fog client sends a connection request to a fog node, which assesses the client's trust score. If the client is deemed trustworthy, the connection is granted; otherwise, it is rejected. Upon granting the connection, the fog node's trust score is

evaluated, and if the node is trustworthy, the connection is established [2,56]. Trust management systems based on the OpenFog [32,57] reference architecture is deployed above the resource management layer and within the support layer, configured accordingly. The architecture of a two-way trust management system in a fog environment is illustrated in Fig. 1 [40]. Each fog node/server is managed by an owner, who may oversee multiple servers [32,40]. The descriptions of all notations used have been compiled in Table 1 to facilitate the reader's understanding.

According to mental logic, the trust of node v is formalized by $\psi_v = (a_v, b_v, c_v, d_v)$ [1,32]. Here, a_v is the belief for the reliability of v (i.e., belief), b_v is the disbelief/doubt for the reliability of v (i.e., disbelief), c_v is the uncertainty for the reliability of v (i.e., uncertainty), and d_v is the prior probability of trustworthiness without evidence for v (i.e., atomicity). According to ψ_v, the trust degree of node v is defined by $P_v = d_v.c_v + a_v$. Let the positive (p) and negative (n) experiences of neighboring nodes be the basis for measuring the trust degree of node v. According to this, $a_v = p/(n+p+1)$, $b_v = n/(n+p+1)$, and $c_v = 1/(n+p+1)$.

Assume that x, y, and z are trustor, trustee, and recommender nodes, respectively [58,59]. Accordingly, x has a subjective trust of z defined by $\psi_{x,z}$, and z has a subjective trust of y defined by $\psi_{z,y}$:

$$\psi_{x,z} = (a_{x,z}, b_{x,z}, c_{x,z}, d_{x,z}) \tag{1}$$

$$\psi_{z,y} = (a_{z,y}, b_{z,y}, c_{z,y}, d_{z,y}) \tag{2}$$

Given $\psi_{x,z}$ and $\psi_{z,y}$, the implicit trust for y by x based on the recommendation of z is computed:

$$\psi_{x,y} = (a_{x,z}.a_{z,y}, a_{x,z}.b_{z,y}, b_{x,z} + c_{x,z} + a_{x,z}.c_{z,y}, d_{z,y}) \tag{3}$$

Let $\psi_{x,y}$ and $\psi_{z,y}$ be the recommendations given by nodes x and z about node y, respectively. The combination of these recommendations for node y:

$$\psi_{xz,y} = \left(\frac{a_{x,z}.c_{z,y} + d_{z,y}.c_{x,y}}{c_{x,y} + c_{z,y} - c_{x,y}.c_{z,y}}, \frac{b_{x,y}.c_{z,y} + b_{z,y}.c_{x,y}}{c_{x,y} + c_{z,y} - c_{x,y}.c_{z,y}}, \frac{c_{x,y}.c_{z,x}}{c_{x,y} + c_{z,y} - c_{x,y}.c_{z,y}}, d_{xz,y}\right) \tag{4}$$

where $d_{xz,y}$ is calculated as follows:

$$d_{xz,y} = \frac{d_{x,y}.c_{z,y} + d_{z,y}.c_{x,y} - (d_{x,y} + d_{z,y}).c_{x,y}.c_{z,y}}{c_{x,y} + c_{z,y} - 2c_{x,y}.c_{z,y}} \tag{5}$$

The final indirect trust for y evaluated by x is:

$$\psi_{x,y}^{Indirect} = (\psi_{x,r_1} \otimes \psi_{r_1,y}) \oplus (\psi_{x,r_2} \otimes \psi_{r_2,y}) \ldots (\psi_{x,r_k} \otimes \psi_{r_k,y}) \tag{6}$$

ERTWT identifies reliable nodes before applying the Ad hoc On-Demand Distance Vector (AODV) protocol to establish routing paths [60,61]. By integrating trust and energy metrics, it optimizes the efficiency and precision of data transmission. Prioritizing nodes with greater energy reserves for routing minimizes the risk of network disruptions and maintains stable data flow [62,63]. In fog computing scenarios, energy consumption occurs across several essential operations [32,64]. The energy consumed by node x to process a packet is defined as follows:

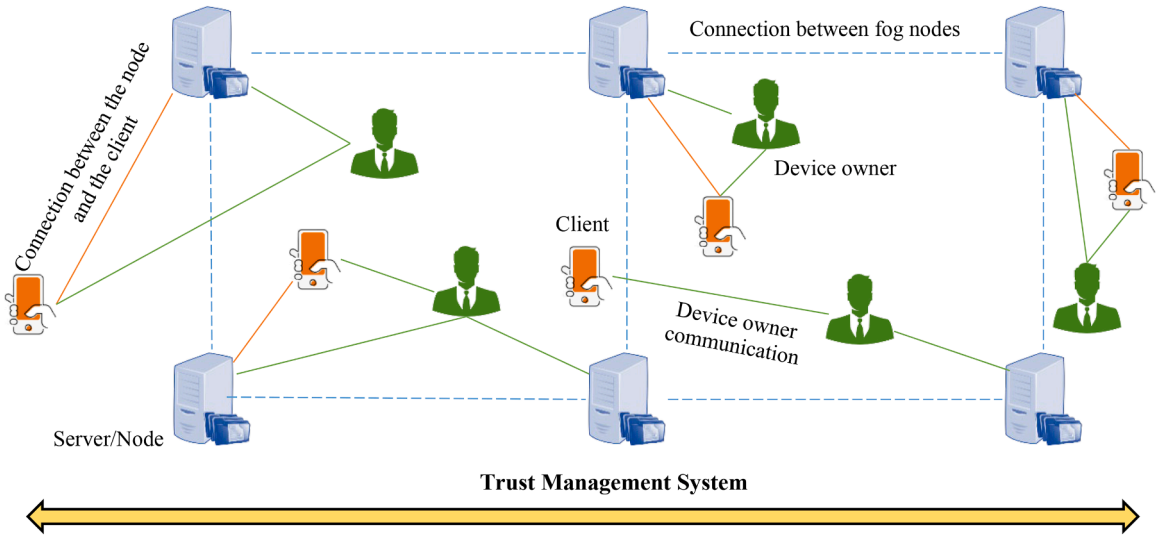


Fig. 1. Two-way trust management system architecture.

Table 1
Description of all the notations.

Notations	Description
ψ_v	Trust node v based on mental logic
a_v	Belief for the reliability of v
b_v	Disbelief/doubt for the reliability of v
c_v	Uncertainty for the reliability of v
d_v	Prior probability of trustworthiness without evidence for v
P_v	Trust degree of node v
$\oplus$	Discounting operator
$\otimes$	Consensus operator
$\psi_{x,y}$	x has a subjective trust of y
ST_x	Overall direct trust score c_x
E_x	Energy consumed by node x
V	Battery voltage of the nodes
n	Number of clients
m	Number of nodes
$c_i \in C$	i-th client from the set of C clients
$f_j \in F$	j-th node from the set of F nodes
I	Matrix of interactions between a node and all clients
R	Matrix of realized interactions between a node and all clients
P	Matrix of propagations made between a node and all clients

$$E_x = E_x^{rx} + E_x^{tx} + E_x^{ls} + E_x^{idle} = V.\left(\frac{\omega.I_x^{rx}}{\rho} + \frac{\omega.I_x^{tx}}{\rho} + t_x^{ls}.I_x^{ls} + t_x^{idle}.I_x^{idle}\right) \tag{7}$$

where E_x^{rx}, E_x^{tx}, E_x^{ls}, and E_x^{idle} are the energy spent by node x in reception, transmission, listening, and idle modes. Here, the symbol I represents the current consumed and the symbol V represents the battery voltage of the nodes. Also, ω and ρ represent the packet length and data rate, respectively. Meanwhile, $t_x^{idle} = 2^{BO} - 2^{SO}$, where BO indicates Beacon Order and SO indicates Superframe Order. Finally, t_x^{idle} is defined as:

$$t_x^{idle} = 2^{BO} - \left(t_x^{rx} + t_x^{tx} + t_x^{idle} + t^*\right) \tag{8}$$

where t^* indicates clear channel assessment.

To estimate the energy consumed by x, we proceed as follows [1]:

$$E_x = \begin{cases} V.\left(\dfrac{\omega.I^{tx}}{\rho} + t_x^{ls}.I^{ls} + t_x^{idle}.I^{idle}\right) & \text{if } x \text{ is source} \\ V.\left(\dfrac{\omega.I^{rx}}{\rho} + t_x^{ls}.I^{ls} + t_x^{idle}.I^{idle}\right) & \text{if } x \text{ is dectination} \end{cases} \tag{9}$$

4. Energy-aware secure routing scheme via two-way trust evaluation

The multipath routing allows for scalable and dependable data exchange. Firstly, the GFlowNets [65] is used to anticipate the nodes' remaining energy. After energy prediction, the trust score of the nodes is calculated based on a two-way model. Finally, multipath routing is performed using the AODV routing protocol, and the ideal transmission path is determined according to the trust score and residual energy. After determining the best transmission path, data forwarding is carried out. In order to prevent message flooding and to shorten the number of nodes between the source and the destination, the route is finally maintained during the route maintenance stage.

The trust matrices and information for trust evaluation are primarily stored and processed at the fog nodes. Each fog node maintains trust information about its associated clients and periodically updates it based on direct and indirect interactions with other nodes. The computational tasks related to trust score calculation, such as energy trust, direct trust, and indirect trust, are executed on the fog nodes to reduce the burden on resource-constrained IoT devices. The base station plays a supervisory role, aggregating trust data from the fog nodes and verifying their reliability. This distributed approach ensures scalability and efficiency in processing the trust metrics without overloading any single entity in the network. Additionally, the GFlowNets is trained and executed on the base station. Once the model is trained, the pre-trained GFlowNets model is deployed on the fog nodes, which utilize it for making routing and trust decisions. This approach ensures that there is no significant computational overhead on the resource-constrained fog nodes, as the heavy computational tasks associated with training GFlowNets are handled at the base station. The fog nodes simply apply the trained model to evaluate trust and make routing decisions efficiently.

4.1. Energy prediction

Predicting the energy consumption of fog nodes is crucial for establishing secure routes in IoT networks, particularly in

environments where energy resources are limited and security threats are prevalent. Fog nodes, acting as intermediaries between IoT devices and cloud servers, are responsible for processing, storing, and transmitting data. However, their energy levels directly impact their ability to perform these tasks efficiently. If a node's energy depletes, it may not only fail to process data effectively but also become vulnerable to security breaches or malicious attacks. By predicting the energy consumption of fog nodes, the routing mechanism can dynamically select paths that not only prioritize secure communication but also ensure that the nodes along the path have sufficient energy to sustain the transmission process. This energy-aware routing helps avoid paths with low-energy nodes that could become compromised or fail during communication, thereby improving the overall reliability and security of the network. Additionally, with better energy predictions, network efficiency is enhanced, as routes are optimized to balance energy consumption and trustworthiness, ultimately leading to prolonged network lifetime and reduced vulnerability to attacks.

We utilize GFlowNets [65] to predict the energy consumption of fog nodes. GFlowNets, with their ability to model complex distributions, allow us to efficiently forecast the energy levels of fog nodes based on their past behavior and current workloads. By incorporating GFlowNets, we enhance both the energy management and security of the IoT network, as low-energy nodes, which are more prone to failure or compromise, are avoided in the routing process. GFlowNets are a class of generative models designed to sample complex structures or sequences by modeling the generation process as a stochastic flow through a directed acyclic graph (DAG). Unlike traditional generative models, which sample data points all at once, GFlowNets generate samples in a step-by-step process, similar to reinforcement learning approaches, where decisions are made incrementally. The key idea behind GFlowNets is to learn a probability distribution over possible sequences or structures, such that the generation of each structure is proportional to its desired reward or likelihood. Let E_x^{rs} denote the residual energy of node x, defined as $1 - E_x$, where E_x signifies the energy expended by node x.

Sampling a compositional object s can be accomplished by a series of stochastic stages, allowing for the representation of complex multimodal distributions $P_T(s)$ over these objects. The sampling policy is designed to ensure that the probability $P_T(s)$ of selecting an object s is roughly proportional to the value $R(s)$ derived from a specified reward function associated with that object. We also discuss a negative reward function $R_N(s) = -\log R(s)$, indicating that the reward function is non-negative and represents an unnormalized probability. Fig. 2 illustrates an example of object building utilizing GFlowNet. Each constructive sequence commences in the singular beginning state s_0 and concludes in a terminal state. Fig. 3 depicts the collection of all trajectories originating from s_0 and concluding in a terminal state s. The term "flow" in "generative flow networks" denotes unnormalized probabilities that can be acquired by GFlowNet learning methodologies. The flow in an intermediate state s is a weighted aggregation of the non-negative rewards from the termination states accessible from s.

To model energy consumption in fog nodes using GFlowNets, the main goal is to design a probabilistic model that captures the energy dynamics of each fog node as it processes and transmits data over time. The GFlowNet will learn to sample energy consumption trajectories (sequences) proportional to a reward function, which in this case, is related to energy efficiency and node reliability. Here, we treat the energy consumption prediction as a flow through a DAG, where each state represents a specific energy level of the fog node, and each action corresponds to a workload or transmission event that consumes energy. Let the energy consumption of a fog node at time t be represented by $E(t)$, which is a function of the node's current load, data transmission, and computational tasks. The GFlowNet generates sequences of energy consumption steps, starting from the initial energy level $E(0)$ and predicting how much energy will be consumed after each task or event until reaching a terminal state $E(T)$, where T is the prediction horizon.

GFlowNets model a forward flow $F(s, a)$ and a backward flow $F(s', a-1)$ between states s and s', where s represents a state cor-

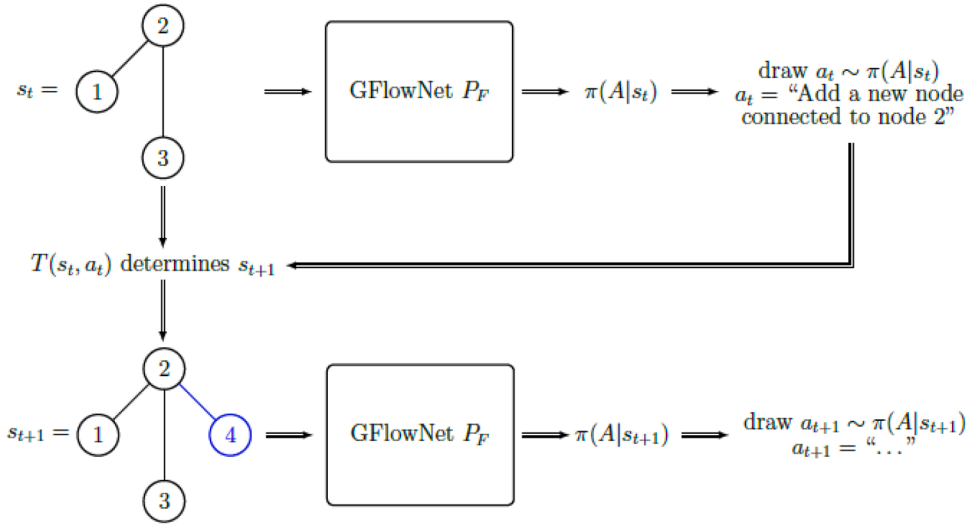


Fig. 2. An example of creating an object by GFlowNet. Here, s_t is the state of the object/node at time t, and a_t is the action performed at time t by GFlowNet to transition to state $s_{t+1} = T(s_t, a_t)$.

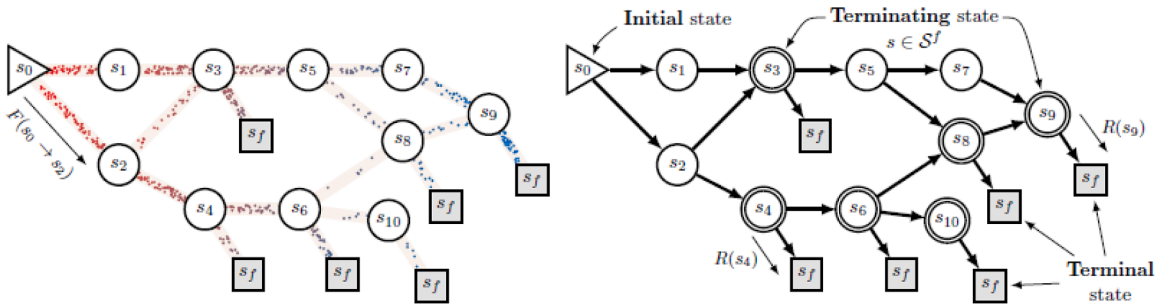


Fig. 3. Schematic of a GFlowNet in state s as a DAG to represent a flow function. Here, the process stops when an action leads to the terminal state s_f, and obtaining the reward $R(s)$. A state can generally be attained by multiple pathways. GFlowNet learns a policy whereby the likelihood of sampling a terminating state is proportional to $R(s)$. It endeavors to learn a flow function $F(s)$ and $F(s{\to}s')$ across all states s and transitions $s{\to}s'$, with $F(s) = R(s)$ at terminal states and $F(s_0)$ representing the cumulative rewards across all terminal states.

responding to a specific energy level of a fog node, a is an action that causes a transition between energy states, such as data processing or packet transmission, and s' represents the energy state after action aaa has been taken. These flows are designed to satisfy a flow consistency condition, which ensures that the probability distribution over energy states is proportional to a predefined reward function $R(s')$, related to the node's energy efficiency and trustworthiness. The GFlowNet learns the optimal distribution over possible energy states s' by maximizing the flow consistency and reward. To predict energy consumption, GFlowNets follow the sequence:

1. State Space S: Define the set of energy levels of the fog node, denoted as $\{E_0, E_2, \ldots, E_T\}$ where E_0 is the initial energy and E_T is the terminal energy level after a series of tasks.
2. Action Space A: The set of actions corresponding to the node's workloads, data transmissions, and computational processes.
3. Transition Probability $P(s'|s,a)$: This models the probability of moving from state s (energy level) to state s' based on action aaa, representing energy consumption during an operation.
4. Reward Function $R(s')$: A reward is associated with the energy state s', reflecting the node's energy efficiency and its trustworthiness in the network.

The energy consumption model can be represented as a step-wise decrease in energy:

$$E_{t+1} = E_t - \Delta E(a_t) \tag{10}$$

where $\Delta E(a_t)$ is the energy consumed by the fog node after performing action a_t, such as processing a data packet or executing a computation task.

The forward flow $F(s,a)$ and backward flow $F(s', a-1)$ are learned to satisfy the flow consistency:

$$\sum_a F(s,a) = \sum_{a^{-1}} F\left(s', a^{-1}\right) = R(s') \tag{11}$$

where the total flow into a state s' must match the reward $R(s')$, which in this case is related to the node's energy efficiency.

The reward $R(s')$ for reaching an energy state s' can be defined as:

$$R(s') = \frac{1}{1 + E(s')} \tag{12}$$

where $E(s')$ is the energy consumed up to state s'. This encourages the GFlowNet to prioritize sequences with lower energy consumption.

The GFlowNet is trained using reinforcement learning or maximum likelihood estimation to sample energy consumption trajectories. It maximizes the likelihood of sequences that correspond to minimal energy consumption while maintaining security. Once trained, the GFlowNet generates energy consumption trajectories for fog nodes, predicting the most likely energy state $E(T)$ after a sequence of operations. This allows the routing algorithm to avoid low-energy nodes and ensure secure, energy-efficient communication in the IoT network. GFlowNets are designed to simulate an edge flow F_θ defined across a graph G, ensuring that the terminal flow corresponds to the reward $R(s)$ and that the flow remains consistent. This is accomplished by establishing a loss function whose global minimum results in the consistency condition. This was initially articulated through a learning aim akin to temporal difference, referred to as flow-matching [65]:

$$\mathscr{L}_{FM}(s;\theta) = \log\frac{\sum_{s' \in Parent(s)} F_\theta(s' \to s)}{\sum_{s'' \in Child(s)} F_\theta(s \to s'')}\Bigg)^2 \tag{13}$$

Bengio et al. [65] demonstrate that trajectories τ_i, sampled from an exploratory training strategy $\overline{\pi}$ with complete support, yield a

consistent edge flow when minimized according to this equation. At this juncture, the forward transition probability defined by this flow $P_{F_\theta}(s'|s)$ would sample objects s with a probability $P_F(s)$ that is proportional to their reward $R(s)$:

$$P_{F_\theta}(s'|s) = \frac{F_\theta(s \to s')}{\sum_{s'' \in Child} F_\theta(s \to s'')} \tag{14}$$

Specifically, the trajectories for training GFlowNets are sampled from an experimental policy that combines the GFlowNet sampler P_{F_θ} with a consistent selection of actions permissible in each state:

$$\overline{\pi}_\theta = (1-\delta)P_{F_\theta} + \delta \cdot \text{Uniform} \tag{15}$$

where δ is an influence coefficient.

4.2. Trust score

A fog environment consists of a set of fog nodes and clients, which are represented by $F = \{f_1, f_2, \ldots, f_m\}$ and $C = \{c_1, c_2, \ldots, c_n\}$, respectively. Here, f_j and c_i are j-th node and i-th client respectively out of m nodes and n clients. Nodes play the role of fog servers and clients play the role of IoT devices. In the theory of mental logic, $\psi_{x,y}$ represents the trust score associated with node c_x calculated by client f_y. If we consider the calculated trust type as k, the symbol $\psi^k_{x,y}$ is used for this definition. Meanwhile, the matrix $I \in \mathbb{R}_{2\times n}$ contains $I_{1,i}$ and $I_{2,i}$ which represents the interactions between nodes and client c_i. The first vector refers to the average interactions and the second vector refers to the total interactions. Similarly, $P \in \mathbb{R}_{2\times n}$ represents the propagations made and $R \in \mathbb{R}_{2\times n}$ represents the interactions realized.

In general, the calculation of two-way trust involves measuring the trust score "for clients by nodes" and "for nodes by clients". Information such as ownership ($\psi^O_{x,y}$), honesty ($\psi^H_{x,y}$), and social relationship ($\psi^F_{x,y}$) are used for the first case and ownership ($\psi^O_{y,x}$), latency ($\psi^L_{y,x}$), and PDR ($\psi^P_{y,x}$) are used for the second case. The direct trust value of a node is assessed by observing the behavior of its neighboring nodes. This trust function is determined by analyzing the packet transmission and reception status of the neighbors. The direct trust between node c_i and its neighboring node c_j can be calculated as follows:

$$\psi^{Direct}_{x,y} = \sigma.HT_{x,y} + (1-\sigma).NT_{x,y} \tag{16}$$

where σ is the influence coefficient, and $HT_{x,y}$ is the historical trust value, which is the result of the evaluation of f_y by c_x in the past. Also, $NT_{x,y}$ is the trust value of f_y's neighbor evaluated by c_x.

$$HT_{x,y} = \psi^O_{x,y} + \psi^H_{x,y} + \psi^F_{x,y} \tag{17}$$

$$NT_{x,y} = \frac{\tau.(rn_y - zn_y) + (sn_y - un_y)}{ln_y} \tag{18}$$

where rn_y and sn_y represent the number of packets received and transmitted by f_y, respectively. Meanwhile, zn_y and un_y indicate instances where f_y declined to receive or send data. Also, τ is a penalty factor designed to hasten the reduction of trust values for nodes that exhibit misbehavior.

$$\tau = \frac{-\rho}{e^{-\frac{MX_j}{NX_j}}} \tag{19}$$

where MX_j represents the proportion of incorrect behavior and NX_j represents the proportion of normal behavior in the previous ten trust estimation processes. Here, ρ is an adaptive parameter to control the rate of change of τ.

In a fog network, the calculation of factors such as ownership, honesty, and social relationships for assessing client trust by nodes is achieved through various methods. Each of these elements contributes to the overall trust score, helping nodes evaluate the reliability and credibility of the clients they engage with. These factors are typically part of a comprehensive trust system that considers the behavior, interactions, and histories of both nodes and clients. Ownership refers to the control or stake that a node has over resources or clients, as shown in Eq. (20). Honesty relates to the integrity of a node in its interactions with clients and other nodes. This can be measured by monitoring the consistency of the information provided by the node, adherence to protocols, and transparency in transactions. Social relationships encompass the connections and interactions between nodes and clients within the network. Nodes that have a positive social network and strong relationships with other trusted entities can enhance their own trust scores.

$$\psi^O_{x,y} = \begin{cases} 0.33 & \text{if } c_x \text{ and } f_y \text{ belong to the same person} \\ 0.2 & \text{otherwise} \end{cases} \tag{20}$$

Indirect trust is measured for a client and target nodes through shared nodes. The common neighbors of c_x and f_y may include both trusted and untrusted nodes. To prevent potential attacks by a third-party node mmm, it is important to filter out untrusted neighboring nodes. The indirect trust of client f_y to node c_x is as follows:

$$\psi_{x,y}^{Indirect} = \sum_{k\in\Delta}\left(\varphi_k.HT_{x,k}, HT_{y,k}\right) \tag{21}$$

where Δ denotes the set of trusted nodes that are mutually shared by both c_x and f_y. On the other hand, φ_k is calculated as follows to improve confidence accuracy:

$$\varphi_k = \frac{HT_{x,k}}{\sum_{l\in\Delta} HT_{x,l}} \tag{22}$$

To ensure strong security and reliable nodes, comprehensive trust integrates both direct and indirect trust to determine whether a node can be considered trustworthy:

$$\psi_{x,y} = \gamma_1.\psi_{x,y}^{Direct} + (1-\gamma_1).\psi_{x,y}^{Indirect} \tag{23}$$

where γ_1 is the influence coefficient.

In the two-way trust system, client c_x must also calculate the trust of node f_y. This approach involves calculating both the direct and indirect trust scores, which are then combined to form an overall trust evaluation. The direct trust score for f_y by c_x is equal to $ST_{y,x} = \psi_{y,x}^{O} + \psi_{y,x}^{L} + \psi_{y,x}^{P}$, which is calculated as follows by considering the definition of subjective logic:

$$\psi_{y,x}^{Direct} = \psi_{y,x}^{Direct} \otimes \left(ST_{y,x} \oplus ST_{x,y}\right) \tag{24}$$

In this study, $\psi_{y,x}^{L}$ includes the time required for f_y to serve c_x, while $\psi_{y,x}^{P}$ denotes the ratio of successfully received packets between c_x and f_y to the total number of packets sent. Meanwhile, $\psi_{y,x}^{O}$ is estimated based on [32]:

$$\psi_{y,x}^{O} = \begin{cases} 0.33 & \textit{if } c_x \textit{ and } f_y \textit{ belong to the same person} \\ 0.2 & \text{otherwise} \end{cases} \tag{25}$$

The influence of indirect trust on the overall trust score is determined by the level of trust previously established in the trusted entity during earlier trust evaluations. The indirect trust score of c_x as evaluated by f_y:

$$\psi_{y,x}^{Indirect} = \frac{\mathcal{N}(rec)}{\max(rec) + \mathcal{N}(rec)}.\sum_{k\in\Delta}\left(\varphi_{\ell}.ST_{x,k}, ST_{y,k}\right) \tag{26}$$

where $\mathcal{N}(rec)$ indicates the number of recommenders and $\max(rec)$ indicates the maximum number of recommenders.

The trust score for nodes is calculated by clients based on various factors such as direct interactions, performance metrics, and feedback from neighboring clients. This evaluation helps clients determine the reliability and trustworthiness of the nodes they interact with in the network. The final trust score for each pair of f_y and c_x considering the coefficient γ_2 is as follows:

$$\psi_{y,x} = \gamma_2.\psi_{y,x}^{Direct} + (1-\gamma_2).\psi_{y,x}^{Indirect} \tag{27}$$

5. Experiments

This section compares the proposed strategy with analogous approaches to validate its efficacy in trust management and enhancing the security of fog environments. The scheme is simulated using MATLAB, and all experiments and comparisons are conducted on a Lenovo Gen 11 Laptop with Intel Corei7–1355 U Processor at 5.0 GHz, 32 GB LPDDR5 Memory, and Windows 11 Pro. The details of the simulation environment and the results of the experiments are given below.

5.1. Experimental setup

Throughout each simulation period, if many trust zones exist within the trajectory, the average trust scores are taken into account. The virtual fog environment is established as per [31,32,40], comprising 200 fog clients, 40 fog servers, and 20 owners. The upper limit of neighboring nodes for trust score recommendations is established at 6 [66,67]. The experiments utilize a total of 25 simulation periods. The default rate for malicious nodes is 15%. In the simulation environment, the number of processor cores for each fog node is randomly selected between 16 and 32, with the processing cost per core ranging from $5 to $10. Each fog node is equipped with storage and memory capacities of 500–1000 GB and 4–8 GB, respectively. The resource usage cost for 100 GB of storage and 1 GB of memory is $7.5. The latency threshold for routing is randomly assigned between 50 ms and 100 ms for each request. Additionally, the demand for processor cores, storage, and memory varies between 1 and 8 cores, 10–50 MB of storage, and 100–400 MB of memory, respectively [68]. On the other hand, the initial energy of the node is equal to 0.5 J, the simulation area is equal to 500 $m \times 500$ m, and the policy of selecting malicious nodes is random.

During network operations, selective forwarding attacks and blackhole attacks are initiated to simulate malicious behavior. Selective forwarding attack and blackhole attack are two critical threats to secure routing in IoT networks and fog computing environments [69,70]. In a selective forwarding attack, a malicious node selectively drops certain packets while forwarding others, making it harder to detect since some traffic still flows through the network. This can degrade network performance and cause significant data

loss [71,72]. In contrast, a blackhole attack involves a malicious node advertising itself as having the shortest route to the destination, only to drop all received packets, completely disrupting the communication flow [73]. Both attacks can severely compromise network security, requiring robust trust-based or cryptographic mechanisms to detect and mitigate such behaviors.

5.2. Benchmark approaches

This study compares the proposed ERTWT with trust-based strategies, including TMS [40], ESFRM [31], MTTM [32], and EASR [35]. The specifics of these schemes are as follows:

- TMS [40]: Two-way trust management system approach
- ESFRM [31]: Efficient and secure fog-based routing mechanism
- MTTM [32]: Modified two-way trust management system
- EASR [35]: Energy aware and secure routing model

5.3. Comparison results

The effectiveness of our proposed scheme is compared against four equivalent and advanced trust-based techniques: TMS, ESFRM, MTTM, and EASR. The convergence of trust in routing schemes for an effective fog node is assessed concerning the trust computation cycles. The default rate of malevolent nodes is established as 15 %, while the influence of direct and indirect trust on overall trust is defined with γ set at 0.6. The calculated trust scores for the different routing schemes in both selective forwarding and blackhole attacks are shown in Fig. 4. The results demonstrate that MTTM and ERTWT, which provide trust management grounded in subjective logic, demonstrate enhanced performance regarding trust convergence and accuracy. Nonetheless, the suggested approach surpasses MTTM owing to its utilization of diverse domains and an energy-conscious two-way trust mechanism, albeit the distinction is minimal. At the same time, ERTWT leverages GFlowNets to predict energy levels, improving data transmission efficiency while maintaining robust security. The trust management model employed by ESFRM demonstrates the weakest performance. TMS, similar to ESFRM, relies on limited parameters for trust calculation, leading to comparable trust scores. However, ESFRM achieves faster convergence than TMS, though it sacrifices accuracy as the number of trust computation cycles increases. On the other hand, the trust value in EASR increases faster compared to ESFRM, TMS, and MTTM in both attacks. The performance of EASR is very effective in detecting and avoiding malicious nodes. However, the changes of the trust value show that EASR requires more rounds to identify malicious nodes compared to our scheme and provides a relatively lower trust value. The suggested scheme offers superior accuracy and rapid convergence time owing to its adaptive and bidirectional characteristics, surpassing conventional different routing schemes.

Fig. 5 depicts the detection rate of malicious nodes in relation to the trust computation cycles employed by current trust management models during selective forwarding and blackhole attacks. In general, the detection rate of malicious nodes increases with increasing cycles. The findings of this experiment demonstrate that the precision in identifying malicious nodes inside our framework is superior. This benefit is ascribed to the detection of hostile nodes using energy-aware routing and the integration of QoS indicators and social links in trust assessment. Moreover, when the cycles of trust computation escalate, the detection rate rises. Overall, the average detection rate for TMS and ESFRM models in selective forwarding attack is 0.613 and 0.555, respectively. These results for blackhole attack are reported as 0.638 and 0.63, respectively. Additionally, the average detection rate for MTTM under selective forwarding and blackhole attacks is 0.65 and 0.672, respectively. On the other hand, the results show that EASR can provide a higher average detection rate under malicious attacks compared to TMS, ESFRM, and MTTM. However, the proposed ERTWT achieves the best performance with an average detection rate of 0.692 and 0.717 in selective forwarding and blackhole attacks, outperforming other routing schemes. The enhanced outcomes underscore ERTWT's effective technique, integrating energy efficiency, QoS, and social trust measurements, which together augment its ability to precisely detect rogue nodes during prolonged computation periods.

Fig. 6 examines the quantity of transmitted packets for the current trust management models. As the frequency of trust computation cycles escalates, the PDR correspondingly rises due to the identification and elimination of additional hostile nodes. The findings illustrate the superiority of our scheme compared to MTTM. This benefit arises from employing GFlowNets to forecast energy consumption and utilizing multiple features for trust assessment, which enable the detection of rogue nodes inside each domain and the transmission of an increased number of packets. The performance of the TMS and EASR routing schemes is slightly better, primarily due to node mobility, which enhances proximity and consequently reduces the overall distance. The analysis of different models shows the superiority of ERTWT with an average PDR of 73.16 and 93.44 for selective forwarding and blackhole attacks, respectively. The average PDRs for the TMS, ESFRM, MTTM, and EASR models under selective forwarding attacks are 68.03, 62.67, 68.88, and 71.67, respectively, and similarly 73.8, 73.15, 82.71, and 90.46 under blackhole attacks. These results clearly demonstrate the superior performance of our proposed scheme. The improved PDRs of ERTWT highlight its effectiveness in precisely detecting and eliminating rogue nodes, thereby facilitating more efficient and reliable packet transport. This is especially important in dynamic contexts where node movement might influence network performance.

Recharging node batteries in hostile and unattended environments is challenging. Consequently, it is a crucial factor to evaluate the energy consumption of nodes during routing to prevent needless energy depletion. The radio energy model of ERTWT incorporates multipath fading and a free space model; the energy expended by node u to transmit x bits of data to node v at a distance d is expressed as Eq. (28). Also, the energy expended at node v to receive x bits of data is calculated as per Eq. (29).

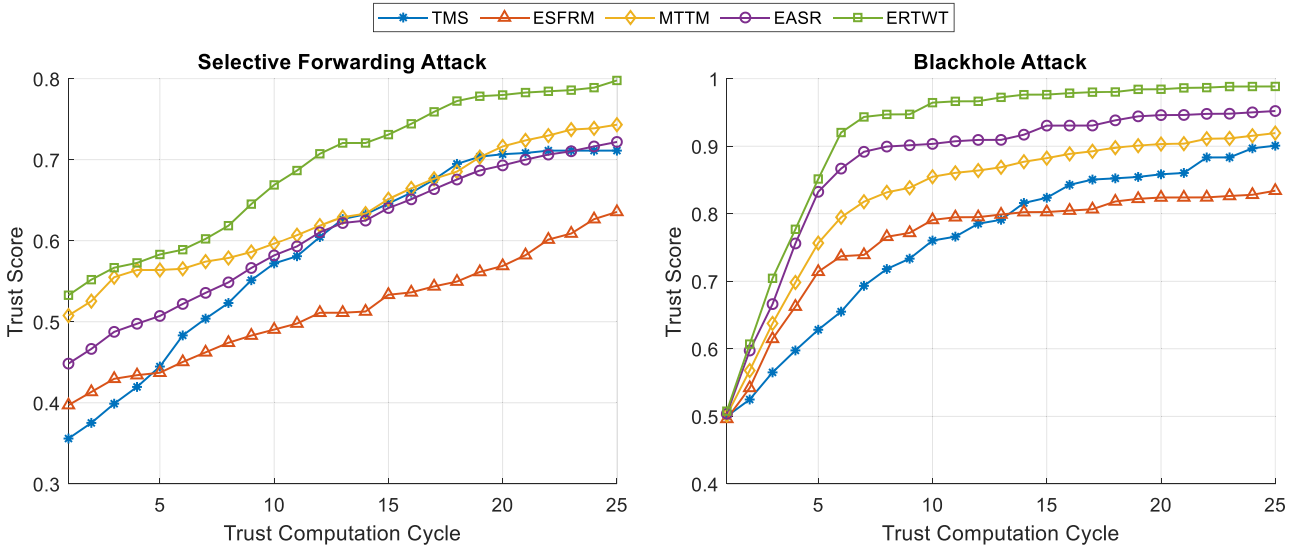


Fig. 4. Trust scores affected by selective forwarding and blackhole attacks in different routing schemes.

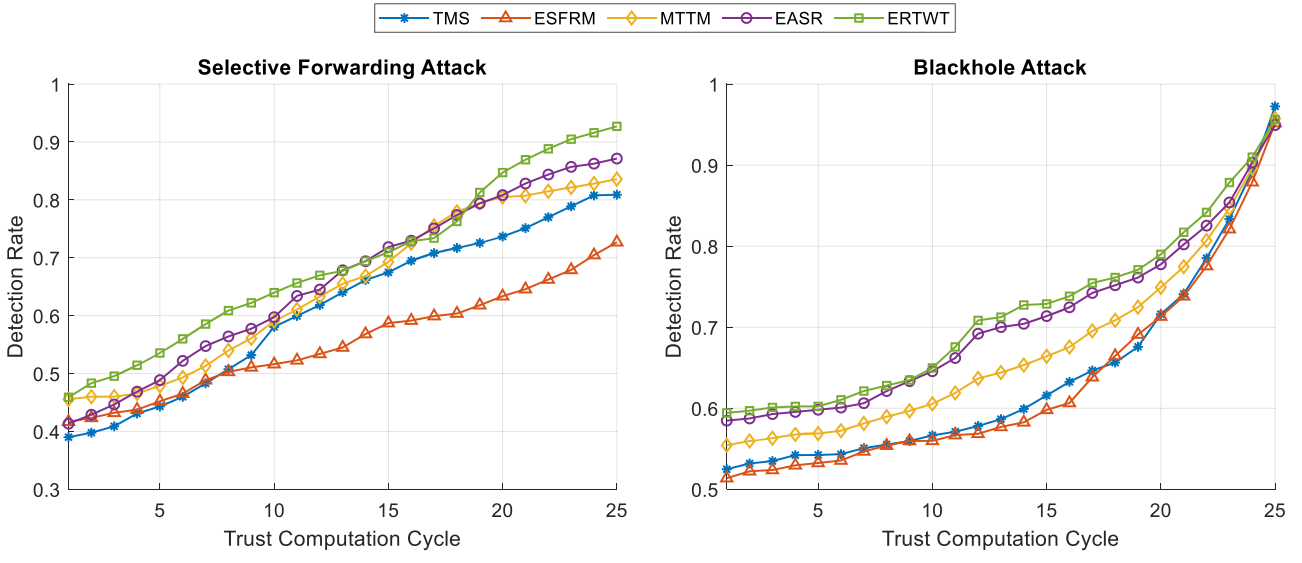


Fig. 5. Average detection rate of malicious nodes affected by selective forwarding and blackhole attacks in different routing schemes.

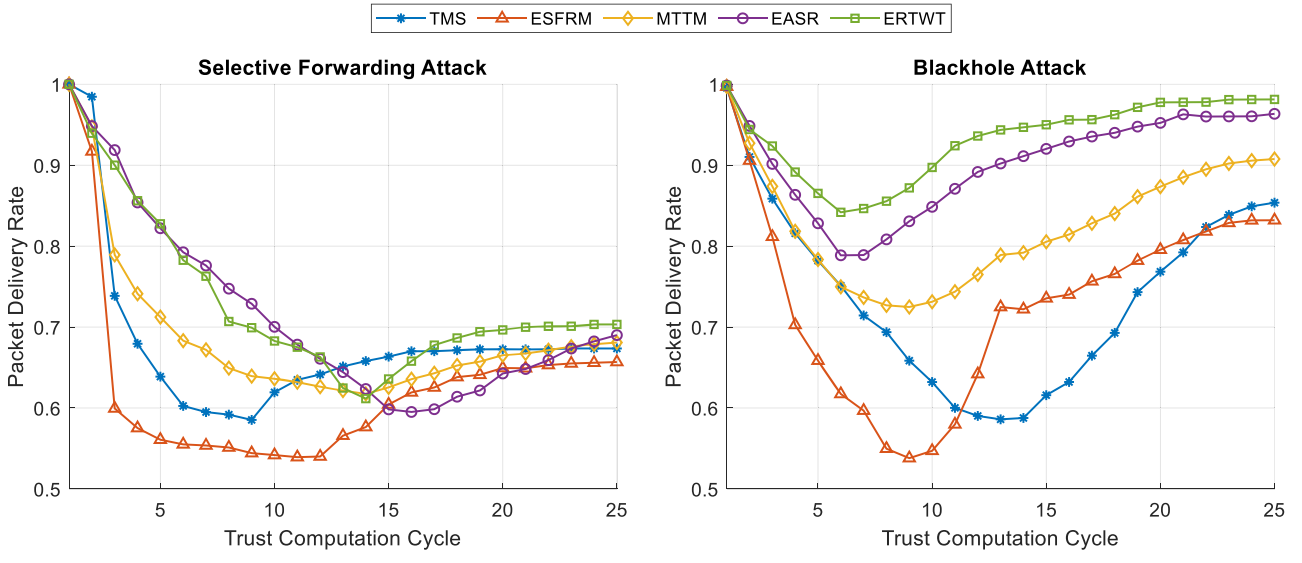


Fig. 6. Analysis of PDR affected by selective forwarding and blackhole attacks in different routing schemes.

$$ET_{u,v} = \begin{cases} x \times E_{elec} + x \times \varepsilon_{f_s} \times d^2 & d < d_0 \\ x \times E_{elec} + x \times \varepsilon_{mp} \times d^4 & \text{otherwise} \end{cases} \tag{28}$$

$$ET_{u,v} = x \times E_{elec} \tag{29}$$

where E_{elec} represents the energy consumed for digital coding and modulation in the electronic circuit, and $d_0 = \sqrt{\varepsilon_{f_s}/\varepsilon_{mp}}$ is the predefined distance threshold. Meanwhile, ε_{f_s} and ε_{mp} are defined as the gain parameters of the transmitter circuit.

Fig. 7 illustrates the energy consumption of network nodes during data transmission between fog nodes and, subsequently, fog clients. The results are reported for both selective forwarding and blackhole attacks, based on an increasing number of cycles. The results show the average residual energy of the entire network. The effectiveness of ERTWT is enhanced by considering both the improved energy threshold and trust scores, where nodes with lower energy consumption and higher trust scores are deemed more secure and thus selected for routing participation. The results show that ERTWT achieves the lowest energy consumption compared to other routing models. The data also explain that the higher rate of data transmission from fog clients to fog nodes in ERTWT is due to a lack of data filtering, leading to increased energy usage. However, during data reception by fog nodes, ERTWT consumes less energy because data filtering is efficiently handled by fog nodes through appropriate computations. Moreover, ERTWT requires fewer cycles to identify malicious nodes with minimal energy loss compared to TMS, ESFRM, MTTM, and EASR.

In another experiment, we have provided the execution time results to demonstrate time complexity and GPU (graphics processing unit) memory results to demonstrate memory complexity, in comparison with other methods. These results are presented in Table 2. Execution time serves as an appropriate measure to demonstrate time complexity, while GPU memory serves as an appropriate measure to demonstrate memory complexity. The ERTWT scheme proposed in this study exhibits superior performance compared to TMS, ESFRM, MTTM, and EASR. Specifically, our scheme shows faster execution times and more efficient GPU memory usage, highlighting its effectiveness in practical implementations. The ERTWT method outperforms other approaches primarily due to its efficient utilization of computational resources. Firstly, it employs a lightweight trust management protocol that minimizes computational overhead, leading to faster execution times. This efficiency is crucial in dynamic environments where rapid decision-making is essential. Secondly, ERTWT optimizes GPU memory usage by leveraging a streamlined data processing pipeline and efficient memory allocation strategies. This approach not only enhances performance but also reduces the energy footprint, making it suitable for resource-constrained IoT environments. Furthermore, the predictive energy consumption model integrated into ERTWT, using GFlowNets, enhances its adaptability and scalability. Since GFlowNets is trained on a standalone server (e.g., base station), there is no significant computational overhead on the resource-constrained fog nodes during the execution of the ERTWT scheme. The fog nodes mainly utilize the pre-trained model in ERTWT, which minimizes the computational burden. This approach ensures that the energy consumption remains within acceptable limits while achieving the desired performance. By accurately predicting energy demands, ERTWT ensures optimal resource allocation and prolongs node lifetimes, thereby improving overall network efficiency. These factors collectively contribute to the superior time and memory complexity performance of the ERTWT method, highlighting its suitability for practical deployment in IoT and edge computing scenarios.

6. Conclusion

One concept that addresses both energy management and security in IoT networks is mutual trust evaluation. In the context of IoT, mutual trust refers to the bi-directional verification process where both the service requester and service provider assess each other's trustworthiness. This evaluation helps ensure that data transmission occurs not only over energy-efficient routes but also over secure and reliable paths. In this paper, we proposed ERTWT as an energy-aware secure routing scheme via two-way trust evaluation for IoT networks to address the dual challenges of energy efficiency and security. By incorporating a comprehensive trust management system that evaluates energy trust, direct trust, and indirect trust, the scheme dynamically selects the most secure and energy-efficient routes. Additionally, the integration of GFlowNets enhances the prediction and optimal utilization of energy levels in nodes. Through two-way trust evaluation, both service requesters and providers can mutually assess each other's trustworthiness, significantly improving network security. The proposed scheme was evaluated against existing energy-aware and trust-based routing protocols, demonstrating superior performance in terms of energy efficiency, malicious node detection, and data transmission rates. Future work will focus on further refining the trust evaluation model and exploring its application to larger-scale IoT environments. Also, we aim to extend our research by experimenting with the proposed model in real-world scenarios to validate its performance under practical conditions.

CRediT authorship contribution statement

Tingxuan Fu: Data curation, Methodology, Validation, Writing – review & editing. **Sijia Hao:** Conceptualization, Data curation, Investigation, Writing – review & editing. **Qiming Chen:** Formal analysis, Funding acquisition, Investigation, Writing – original draft. **Zihan Yan:** Data curation, Resources, Supervision, Validation, Writing – review & editing. **Huawei Liu:** Data curation, Methodology, Writing – original draft, Writing – review & editing. **Amin Rezaeipanah:** Writing – review & editing, Validation, Methodology, Investigation, Data curation.

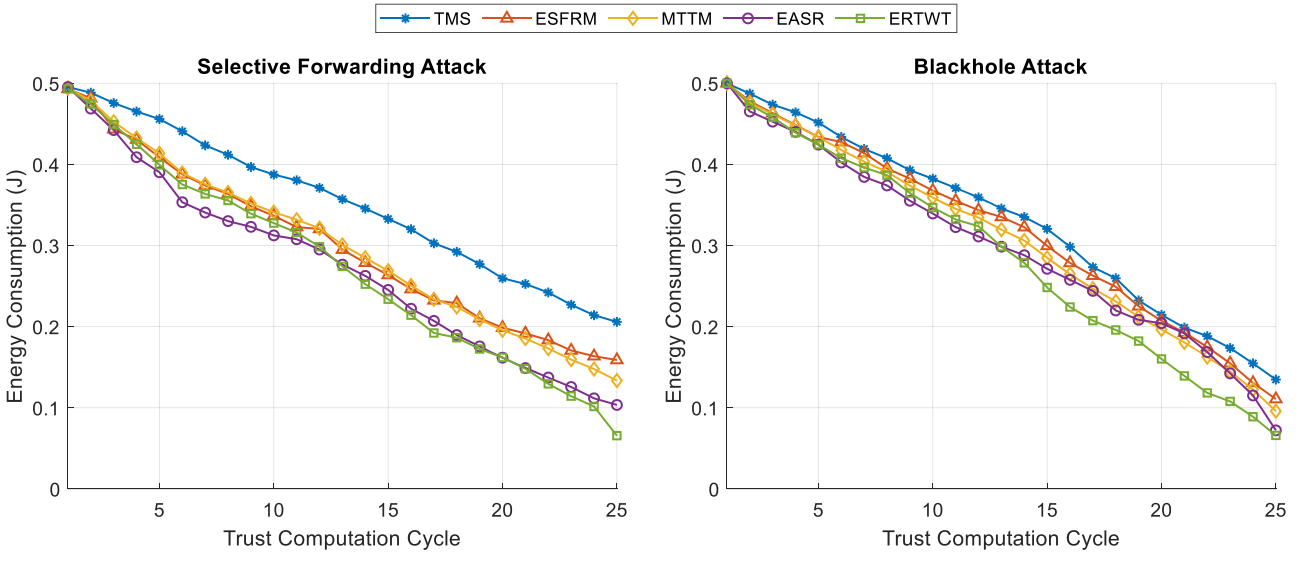


Fig. 7. Analysis of energy consumption affected by selective forwarding and blackhole attacks in different routing schemes.

Table 2
Running time and GPU memory cost for different routing schemes.

Attacks	Metric	TMS	ESFRM	MTTM	EASR	ERTWT
Selective forwarding	Runtime (s)	37.00	42.11	35.86	33.07	31.47
	GPU memory cost	8.43	7.70	6.36	6.19	5.37
Blackhole	Runtime (s)	31.46	37.12	30.85	36.47	28.07
	GPU memory cost	6.25	5.57	4.28	5.16	4.16

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] Y. Zhang, Y. Yu, W. Sun, Z. Cao, Towards an energy-aware two-way trust routing scheme in fog computing environments, Telecommun. Syst. (2024), https://doi.org/10.1007/s11235-024-01226-2.
[2] M. Arazzi, S. Nicolazzo, A. Nocera, A novel IoT trust model leveraging fully distributed behavioral fingerprinting and secure delegation, Pervasive Mob. Comput. 99 (2024) 101889.
[3] G. Arulselvan, A. Rajaram, Hybrid trust-based secure routing protocol for detection of routing attacks in environment monitoring over MANETs, *J. Intell. Fuzzy Syst.*, (Preprint) (2023) 1–16.
[4] L. Tang, L. Zhang, N. Xu, Optimized backstepping-based finite-time containment control for nonlinear multi-agent systems with prescribed performance, Optim. Control Applic. Methods 45 (5) (2024) 2364–2382.
[5] B. Zhu, L. Zhang, B. Niu, N. Zhao, Adaptive reinforcement learning for fault-tolerant optimal consensus control of nonlinear canonical multiagent systems with actuator loss of effectiveness, IEEe Syst. J. 18 (3) (2024) 1681–1692.
[6] X. Wu, S. Ding, B. Niu, N. Xu, X. Zhao, Predefined-time event-triggered adaptive tracking control for strict-feedback nonlinear systems with full-state constraints, Int. J. Gen. Syst. 53 (3) (2024) 352–380.
[7] E. Khezri, E. Zeinali, H. Sargolzaey, SGHRP: secure Greedy Highway Routing Protocol with authentication and increased privacy in vehicular ad hoc networks, PLoS. One 18 (4) (2023) e0282031.
[8] C. Zhang, D. Liu, X. Zhang, C. Spencer, M. Tang, J. Zeng, X. Kong, Hafnium isotopic disequilibrium during sediment melting and assimilation, Geochem. Perspect. Lett. 12 (2020) 34–39.
[9] Y. Gong, H. Yao, A. Nallanathan, Intelligent sensing, communication, computation and caching for satellite-ground integrated networks, IEEE Netw. 38 (4) (2024) 9–16.
[10] T. Wang, G. Zong, X. Zhao, N. Xu, Data-driven-based sliding-mode dynamic event-triggered control of unknown nonlinear systems via reinforcement learning, Neurocomputing. 601 (2024) 128176.
[11] Z. Liu, G. Jiang, W. Jia, T. Wang, Y. Wu, Critical density for k-coverage under border effects in camera sensor networks with irregular obstacles existence, IEEe Internet. Things. J. 11 (4) (2023) 6426–6437.
[12] A.R. Al-Ali, R. Gupta, I. Zualkernan, S.K. Das, Role of IoT technologies in big data management systems: a review and Smart Grid case study, Pervasive Mob. Comput. (2024) 101905.
[13] B. Bi, D. Huang, B. Mi, Z. Deng, H. Pan, Efficient LBS security-preserving based on NTRU oblivious transfer, Wirel. Pers. Commun. 108 (4) (2019) 2663–2674.
[14] Z. Xiao, J. Shu, H. Jiang, G. Min, H. Chen, Z. Han, Overcoming occlusions: perception task-oriented information sharing in connected and autonomous vehicles, IEEE Netw. 37 (4) (2023) 224–229.
[15] D. Zhou, M. Sheng, C. Bao, Q. Hao, S. Ji, J. Li, 6G Non-terrestrial networks-enhanced IoT service coverage: injecting new vitality into ecological surveillance, IEEE Netw. 38 (4) (2024) 63–71.
[16] C. Thai, V.N.Q. Bao, U.H.T. Thai, Security for multi-hop communication of two-tier wireless networks with different trust degrees, REV J. Electr. Commun. 12 (2023) 3–4.
[17] S. Zhang, T. Li, S. Hui, G. Li, Y. Liang, L. Yu, Y. Li, Deep transfer learning for city-scale cellular traffic generation through urban knowledge graph, in: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2023, pp. 4842–4851.
[18] Y. Yang, F. Bai, Z. Yu, T. Shen, Y. Liu, B. Gong, An anonymous and supervisory cross-chain privacy protection protocol for zero-trust IoT application, ACM Trans. Sens. Netw. 20 (2) (2024) 1–20.
[19] X. Hou, L. Xin, Y. Fu, Z. Na, G. Gao, Y. Liu, T. Chen, A self-powered biomimetic mouse whisker sensor (BMWS) aiming at terrestrial and space objects perception, Nano Energy 118 (2023) 109034.
[20] W. Tian, Y. Zhao, R. Hou, M. Dong, K. Ota, D. Zeng, J. Zhang, A centralized control-based clustering scheme for energy efficiency in underwater acoustic sensor networks, IEEe Trans. Green. Commun. Netw. 7 (2) (2023) 668–679.
[21] A.B. Hajirabe, D. Saravanan, C. Jayapratha, S. Parasuraman, A. Manimaran, Trust based security model for intrusion detection in wireless sensor networks, Rivista Italiana di Filosofia Analitica Junior 14 (2) (2023) 985–996.
[22] E. Wang, Y. Yang, J. Wu, W. Liu, X. Wang, An efficient prediction-based user recruitment for mobile crowdsensing, IEEe Trans. Mob. Comput. 17 (1) (2017) 16–28.
[23] Y. Wang, R. Xiao, N. Xiao, Z. Wang, L. Chen, Y. Wen, P. Li, Wireless multiferroic memristor with coupled giant impedance and artificial synapse application, Adv. Electron. Mater. 8 (10) (2022) 2200370.
[24] H. Fang, S. Ma, J. Wang, L. Zhao, F. Nie, X. Ma, L. Zheng, Multimodal in-sensor computing implemented by easily-fabricated oxide-heterojunction optoelectronic synapses, Adv. Funct. Mater. (2024) 2409045, https://doi.org/10.1002/adfm.202409045.
[25] Liu, S., Xu, N., Zhao, N., & Zhang, L. Observer-based optimal fault-tolerant tracking control for input-constrained interconnected nonlinear systems with mismatched disturbances. *Optim. Control Applic. Methods*.doi: 10.1002/oca.3173.
[26] M. Li, H. Cui, C. Liu, C. Shan, X. Du, M. Guizani, A four-dimensional space-based data multi-embedding mechanism for network services, IEEE Trans. Netw. Serv. Manag. 21 (3) (2023) 2741–2750.
[27] W. Fang, W. Zhang, W. Chen, Y. Liu, C. Tang, TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing, Wirel. Netw. 26 (5) (2020) 3169–3182.

[28] H. Li, C. Xia, T. Wang, Z. Wang, P. Cui, X. Li, Grass: learning spatial–temporal properties from chainlike cascade data for microscopic diffusion prediction, IEEE Trans. Neural Netw. Learn. Syst. (2023), https://doi.org/10.1109/TNNLS.2023.3293689.
[29] B. Jiang, Y. Zhao, J. Dong, J. Hu, Analysis of the influence of trust in opposing opinions: an inclusiveness-degree based Signed Deffuant–Weisbush model, Inf. Fusion 104 (2024) 102173.
[30] S. Usturge, T. Pavan Kumar, DEroute: trust-aware data routing protocol based on encryption and fuzzy concept for MANET secure communication in Iot, Inf. Secur. J. 32 (5) (2023) 331–346.
[31] T.S. Malik, J. Tanveer, S. Anwar, M.R. Mufti, H. Afzal, A. Kim, An Efficient and Secure Fog Based Routing Mechanism in IoT Network, Mathematics 11 (17) (2023) 3652.
[32] E. Alemneh, S.M. Senouci, P. Brunet, T. Tegegne, A two-way trust management system for fog computing, Fut. Gener. Comput. Syst. 106 (2020) 206–220.
[33] R. Anitha, B.T. Bapu, P.G. Kuppusamy, N. Partheeban, A.N. Sasikumar, FEBSRA: fuzzy trust based energy aware balanced secure routing algorithm for secured communications in WSNs, Wirel. Pers. Commun. 125 (1) (2022) 63–86.
[34] X. Fu, P. Pace, G. Aloi, A. Guerrieri, W. Li, G. Fortino, Tolerance analysis of cyber-manufacturing systems to cascading failures, ACM. Trans. Internet. Technol. 23 (4) (2023) 1–23.
[35] V. Prasad, H.R. Roopashree, Energy aware and secure routing for hierarchical cluster through trust evaluation, Measurement 33 (2024) 101132.
[36] C. Wahi, S. Chakraverty, V. Bhattacherjee, A trust-based secure AODV routing scheme for MANET, Int. J. Ad Hoc Ubiquitous Comput. 38 (4) (2021) 231–247.
[37] X. Shen, H. Jiang, D. Liu, K. Yang, F. Deng, J.C. Lui, J. Luo, PupilRec: leveraging pupil morphology for recommending on smartphones, IEEe Internet. Things. J. 9 (17) (2022) 15538–15553.
[38] Z. Xiao, H. Fang, H. Jiang, J. Bai, V. Havyarimana, H. Chen, L. Jiao, Understanding private car aggregation effect via spatio-temporal analysis of trajectory data, IEEE Trans. Cybern. 53 (4) (2021) 2346–2357.
[39] B. Hammi, S. Zeadally, H. Labiod, R. Khatoun, Y. Begriche, L. Khoukhi, A secure multipath reactive protocol for routing in IoT and HANETs, Ad Hoc Netw. 103 (2020) 102118.
[40] J. Wang, Z. Luo, C. Wang, A two-way trust routing scheme to improve security in fog computing environment. Cluster Comput., 2024, https://doi.org/10.1007/s10586-024-04621-1.
[41] N.B. Bakhtiari, M. Rafighi, R. Ahsan, A trust management system for fog computing using improved genetic algorithm, J. Supercomput. 80 (2024) 20923–20955.
[42] A. Rehman, K.A. Awan, I. Ud Din, A. Almogren, M. Alabdulkareem, FogTrust: fog-integrated multi-leveled trust management mechanism for internet of things, Technologies. (Basel) 11 (1) (2023) 27.
[43] X. Zheng, S. Yang, X. Wang, A reliable and decentralized trust management model for fog computing in industrial iot, in: NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2023, pp. 1–6.
[44] R. Yadav, G. Baranwal, ReTREM: a responsibility based trust revision model for determining trustworthiness of fog nodes, Comput. Commun. 197 (2023) 159–172.
[45] Y. Liu, Z. Jia, Z. Jiang, X. Lin, J. Liu, Q. Wu, W. Susilo, BFL-SA: blockchain-based federated learning via enhanced secure aggregation, J. Syst. Arch. 152 (2024) 103163.
[46] M. Zhang, E. Wei, R. Berry, J. Huang, Age-dependent differential privacy, IEEe Trans. Inf. Theory. 70 (2) (2023) 1300–1319.
[47] A. Rezaeipanah, E. Afsoon, G. Ahmadi, Improving the performance of intrusion detection systems using the development of deep neural network parameters, in: 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), IEEE, 2020, pp. 278–283.
[48] G. Sun, Y. Zhang, D. Liao, H. Yu, X. Du, M. Guizani, Bus-trajectory-based street-centric routing for message delivery in urban vehicular ad hoc networks, IEEe Trans. Veh. Technol. 67 (8) (2018) 7550–7563.
[49] Q. Cai, J. Chen, D. Luo, G. Sun, H. Yu, M. Guizani, Deter-Pay: a deterministic routing protocol in concurrent payment channel network, IEEe Internet. Things. J. (2024), https://doi.org/10.1109/JIOT.2024.3416086.
[50] B. Ali, M.A. Gregory, S. Li, O.A. Dib, Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in multi-access edge computing, Comput. Netw. 241 (2024) 110197.
[51] M.A. Samsuden, N.M. Diah, N.A. Rahman, A review paper on implementing reinforcement learning technique in optimising games performance, in: 2019 IEEE 9th international conference on system engineering and technology (ICSET), IEEE, 2019, pp. 258–263.
[52] G. Sun, Y. Zhang, H. Yu, X. Du, M. Guizani, Intersection fog-based distributed routing for V2V communication in urban vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 21 (6) (2019) 2409–2426.
[53] Y. Zhong, L. Chen, C. Dan, A. Rezaeipanah, A systematic survey of data mining and big data analysis in internet of things, J. Supercomput. 78 (17) (2022) 18405–18453.
[54] L. Bai, P. Han, J. Wang, J. Wang, Throughput maximization for multipath secure transmission in wireless Ad-Hoc networks, IEEE Trans. Commun. (2024), https://doi.org/10.1109/TCOMM.2024.3409539.
[55] Y. Zhang, F. Zhang, S. Tong, A. Rezaeipanah, A dynamic planning model for deploying service functions chain in fog-cloud computing, J. King Saud Univ.-Comput. Inf. Sci. 34 (10) (2022) 7948–7960.
[56] G. Sun, L. Song, H. Yu, V. Chang, X. Du, M. Guizani, V2V routing in a VANET based on the autoregressive integrated moving average model, IEEe Trans. Veh. Technol. 68 (1) (2018) 908–922.
[57] J. Tan, L. Liu, F. Li, Z. Chen, G.Y. Chen, F. Fang, J. Guo, M. He, X. Zhou, Screening of endocrine disrupting potential of surface waters via an affinity-based biosensor in a rural community in the Yellow River Basin, China, Environ. Sci. Technol. 56 (20) (2022) 14350–14360.
[58] X. Zhang, Y. Li, Z. Xiong, Y. Liu, S. Wang, D. Hou, A resource-based dynamic pricing and forced forwarding incentive algorithm in socially aware networking, Electronics (Basel) 13 (15) (2024) 3044.
[59] H. Zhao, H. Wang, X. Chang, A.M. Ahmad, X. Zhao, Neural network-based adaptive critic control for saturated nonlinear systems with full state constraints via a novel event-triggered mechanism, Inf. Sci. (Ny) 675 (2024) 120756.
[60] Q. Chen, L. Yang, Y. Zhao, Y. Wang, H. Zhou, X. Chen, Shortest path in LEO satellite constellation networks: an explicit analytic approach, IEEE J. Sel. Areas Commun. 42 (5) (2024) 1175–1187.
[61] X. Hou, L. Zhang, Y. Su, G. Gao, Y. Liu, Z. Na, T. Chen, A space crawling robotic bio-paw (SCRBP) enabled by triboelectric sensors for surface identification, Nano Energy 105 (2023) 108013.
[62] K. Ma, J. Yang, P. Liu, Relaying-assisted communications for demand response in smart grid: cost modeling, game strategies, and algorithms, IEEE J. Sel. Areas Commun. 38 (1) (2019) 48–60.
[63] W. Huang, T. Li, Y. Cao, Z. Lyu, Y. Liang, L. Yu, Y. Li, Safe-NORA: safe reinforcement learning-based mobile network resource allocation for diverse user demands, in: Proceedings of the 32nd ACM International Conference on Information and Knowledge Management, 2023, pp. 885–894.
[64] M. Rajasekaran, A. Ayyasamy, R. Jebakumar, Performance and evaluation of location energy aware trusted distance source routing protocol for secure routing in WSNs, Indian J. Sci. Technol. 13 (39) (2020) 4092–4108.
[65] E. Bengio, M. Jain, M. Korablyov, D. Precup, Y. Bengio, Flow network based generative models for non-iterative diverse candidate generation, Adv. Neural Inf. Process. Syst. 34 (2021) 27381–27394.
[66] Y. Gong, H. Yao, Z. Xiong, C.P. Chen, D. Niyato, Blockchain-aided digital twin offloading mechanism in space-air-ground networks, IEEe Trans. Mob. Comput. (2024), https://doi.org/10.1109/TMC.2024.3455417.
[67] H. Zhang, Q. Zou, Y. Ju, C. Song, D. Chen, Distance-based support vector machine to predict DNA N6-methyladenine modification, Curr. Bioinform. 17 (5) (2022) 473–482.
[68] C. Cao, J. Wang, D. Kwok, F. Cui, Z. Zhang, D. Zhao, Q. Zou, webTWAS: a resource for disease candidate susceptibility genes identified by transcriptome-wide association study, Nucleic Acids Res. 50 (D1) (2022) D1123–D1130.

[69] M. Dai, L. Luo, J. Ren, H. Yu, G. Sun, PSACCF: prioritized online slice admission control considering fairness in 5G/B5G networks, IEEe Trans. Netw. Sci. Eng. 9 (6) (2022) 4101–4114.
[70] J. Luo, C. Zhao, Q. Chen, G. Li, Using deep belief network to construct the agricultural information system based on Internet of Things, J. Supercomput. 78 (1) (2022) 379–405.
[71] Z. Liu, J. Feng, L. Uden, Technology opportunity analysis using hierarchical semantic networks and dual link prediction, Technovation 128 (2023) 102872.
[72] X. Wu, S. Ding, N. Xu, B. Niu, X. Zhao, Periodic event-triggered bipartite containment control for nonlinear multi-agent systems with iuput delay, Int. J. Syst. Sci. 55 (10) (2024) 2008–2022.
[73] S. Huang, G. Zong, N. Xu, H. Wang, X. Zhao, Adaptive dynamic surface control of MIMO nonlinear systems: A hybrid event triggering mechanism, Int. J. Adapt. Control Signal Process. 38 (2) (2024) 437–454.