Hindawi
Security and Communication Networks
Volume 2021, Article ID 3717702, 13 pages
https://doi.org/10.1155/2021/3717702

Research Article

Blockchain-Based Key Management and Green Routing Scheme for Vehicular Named Data Networking

Hao Liu,[1] Rongbo Zhu ,[2] Jun Wang,[1] and Wengang Xu[1]

[1]*College of Computer Science, South-Central University for Nationalities, Wuhan 430074, China*
[2]*College of Informatics, Huazhong Agricultural University, Wuhan 430070, China*

Correspondence should be addressed to Rongbo Zhu; rongbozhu@163.com

Received 7 April 2021; Revised 13 June 2021; Accepted 30 June 2021; Published 8 July 2021

Academic Editor: Jie Cui

Due to the distributed and dynamic characteristics of the Internet of Vehicles (IoV) and the continuous growth in the number of devices, content-centric decentralized vehicular named data networking (VNDN) has become more suitable for content-oriented applications in IoV. However, the existing centralized architecture is prone to the failure of single points, which results in trust problems in key verification between cross-domain nodes and consuming more power and reducing the lifetime. Focusing on secure key management and power-efficient routing, this article proposes a blockchain-based key management and green routing scheme for VNDN. A blockchain-based key management scheme is presented to achieve secure and efficient distribution and verification of keys. Specifically, all trusted agencies (TAs) form a consortium blockchain for storing public key hashes to ensure the authenticity of users' public keys. A green global routing scheme based on node relaying pressure (GGNRP) is proposed to save power consumption and reduce the forwarding delay. A new node relay pressure metric is introduced to assist with routing decisions. Detailed experiments and analysis show that, compared with the existing scheme, the proposed scheme can achieve secure key management and GGNRP can decrease the power consumption and average delay by 15.8% and 63.2%, respectively.

1. Introduction

Internet of Vehicles (IoV) is the backbone network of future intelligent transportation systems, and it promises to improve overall traffic efficiency and road safety by enabling the interaction of recreational and safety information through vehicle-to-everything (V2X) communication [1]. To date, vehicles in IoV have relied on IP addresses to find terminals and establish end-to-end communication, regardless of the type of application [2]. Due to the distributed operation, limited bandwidth, and high-speed mobility of nodes and the dynamic network topology of IoV, it is difficult for IoV network links to maintain robustness, durability, and stability [3, 4]. In addition, as the number of Internet of Things (IoT) devices continues to grow, IP addresses are becoming increasingly scarce, making it very difficult to assign IP addresses to IoV devices with high mobility [5]. As a result, a large gap is created between host-based TCP/IP architectures and content-centric IoV applications. Since most of the communication between vehicles focuses on the content rather than the content carrier, the combination of IoV and named data networking (NDN) becomes possible, resulting in vehicular named data networking (VNDN) [6].

NDN is an important candidate for next-generation Internet architecture, where everything, including hosts and data, is named according to hierarchical naming rules. These names replace the role of IP addresses and data transmission switches from a host-to-host approach to data-oriented communication [7]. In addition, NDN caches content in network routers, which allows content requests to be satisfied at the edge of the network, thereby greatly reducing the delay of content delivery [8]. Therefore, NDN is very suitable for providing a reliable transmission solution for IoV communications with high mobility and intermittent connections. However, because of the data-centric feature of NDN, secure communication in NDN has new security requirements [9]. In the content-centric IoV, vehicles may request traffic information (e.g., traffic accident information and road information) for efficient data sharing to optimize road utilization. However, malicious nodes in VNDN may

spread false information to cause traffic congestion or accidents [10]. Therefore, consumers in IoV should care not only about the sender of the data request but also about the producer of the data packet. The packet must be published by an authenticated producer and be unable to be modified by other producers.

To verify the producer's identity information and data integrity, the producer should sign the content so that the name can be effectively and safely bound to the data. In this way, consumers and routers can verify the signature and determine the source of the data, which allows consumers to trust the received data packets. Most existing NDNs use a hierarchical key trust model [11], in which the root key is used as a well-known trust anchor to provide a digital signature on the domain secret key. The key of each domain digitally signs the public key of the user in the domain, and then the user key signs the public key of its device and application. To verify the authenticity of the public key, one can retrieve the secret key chain using the key name. In principle, this method avoids the generation of false messages, but in the application of IoV, there are still some challenges [12]: (1) as a centralized service centre, the root key may be subject to attacks and tampering, which can lead to a single point of failure. Especially in the case of cross-domain key verification, since each domain is relatively independent, it is difficult for each domain to verify the authenticity of the keys issued by the other domains without a trust anchor; (2) since verification needs to traverse the secret key chain, the process of retrieval and verification requires considerable additional overhead, which cannot meet the low-delay requirements of IoV.

On the other hand, the successful implementation of IoV requires a large number of wireless sensors to form a wireless sensor network (WSN) for efficient and fast information transfer. However, the sensors have limited energy and cannot be recharged once they are deployed [13, 14]. The higher the energy efficiency is, the longer the running time of WSN is. The research results show that communication consumes the most energy among many factors that consume energy in WSN [15]. While routing determines the forwarding path between the sender and receiver, effective routing minimizes the communication cost and maximizes the survival time of the wireless sensor network.

In recent years, blockchain technology has been widely used in different fields, such as public key infrastructure (PKI), domain name server (DNS), and IoV [16]. Blockchain ensures that data can be tracked and cannot be easily tampered with through distributed data storage and consensus mechanisms, which guarantees the integrity and authenticity of the participating nodes. To improve the information transmission of blockchain nodes, the combination scheme of blockchain and VNDN was proposed [17]. Therefore, this article proposes a blockchain-based key management and green routing scheme for VNDN, which aims to achieve safe and reliable VNDN key authentication and management while maximizing the use time of wireless sensors. First, a blockchain-based key management scheme is designed to set the management node of each domain as a blockchain node and use blockchain to manage the public keys of different domains to avoid network paralysis due to the failure of a single point. Second, to prevent the premature death of nodes close to the base station (BS) and prolong the survival time of sensors, the concept of node relay pressure is proposed, and a green global routing scheme based on node relaying pressure (GGNRP) is designed. In GGNRP, the source node obtains a green global route for data transmission based on the node-to-BS path information and node energy information stored in the BS, which avoids the routing hole problem that is widely found in planar routing.

The contributions of this article are summarized as follows:

(1) In this article, a blockchain-based key management scheme is proposed to solve the mutual trust problem between different domain nodes. The scheme reduces the number of signature verifications and shortens the time delay of key acquisition and verification, making the NDN more suitable for IoV.

(2) To reduce the transmission delay of VNDN, a green global routing scheme based on node relaying pressure is designed. This scheme uses the path transmission delay and the node relaying pressure value as metrics for routing decisions, which ensures low delay while protecting the nodes with high communication load and low residual energy in VNDN.

The rest of this article is organized as follows. Related work is presented in Section 2. Section 3 details the proposed blockchain-based key management scheme. GGNRP is presented in Section 4. The experimental results are presented in Section 5, followed by the conclusions in Section 6.

2. Related Work

2.1. Security in NDN. NDN is expected to change the architecture of the Internet. For this reason, researchers hope to introduce NDN into IoV to enhance the scalability, reliability, and security of IoV [18]. However, the security requirements of IoV are still difficult to meet due to the high dynamic topology, high mobility, delay, and propagation content [19]. On the other hand, NDN still has various security and privacy issues [20], such as naming, signature, and cache privacy, which makes the establishment of VNDN challenging. Several works have designed solutions to address security issues from the perspective of NDNs [21–23]. Song et al. [21] proposed a smart contract-based trusted content retrieval mechanism for NDNs. This mechanism uses smart contract-based content and a repository of information trusted by producers and provides content retrieval and name resolution services for content consumers. A blockchain-based effective identifier management scheme in the NDN environment was proposed in [22]. This scheme uses the content name of an identifier to create transactions to protect the identifier of a specific user and realizes secure storage and management through this identifier segmentation management technology. A blockchain-based

hierarchical identity-based security mechanism was proposed for NDN to maintain data-oriented authentication [23]. However, most of the existing solutions do not take into account the characteristics of IoV, making them inapplicable in high mobility and low-delay IoV.

For IoV, most existing schemes focus on routing and relaying [24, 25]. To maximize the possibility for users to retrieve the desired content, Mauri et al. [24] formulated this problem as an integer linear programming (ILP) problem and showed how to optimally distribute content in IoV while considering the available storage capacity and available link capacity. In [25], an active data distribution scheme was proposed to push key content to one-hop neighbors in VNDN.

Focusing on information security and privacy preservation in vehicular ad hoc networks, a full session key agreement scheme was proposed based on chaos mapping [26]. To achieve fast authentication during the message verification process, a novel Chinese remainder theorem (CRT)-based conditional privacy-preserving authentication scheme was presented [27]. To manage keys efficiently, a scalable solution was proposed for key and trust management of devices [28], with the combination of blockchain and software-defined networking (SDN) that is able to store the public keys of devices on the blockchain and route the network traffic efficiently. To address the low security and communication efficiency in the blockchain, a key secret-sharing scheme was proposed based on generative adversarial networks (GANs), which view the secret as an image during the secret-sharing process [29]. However, since the security aspects of VNDNs have not been extensively studied, communication in IoV can be subject to many security threats, such as denial of service (DoS) attacks, worm attacks, disinformation attacks, replay attacks, timing attacks, single points of failure, and content poisoning attacks.

2.2. Green Routing Protocol. According to the network structure, the existing green routing protocols can be divided into two types. One type is hierarchical routing, such as the low-energy adaptive clustering hierarchy (LEACH) [30], power-efficient gathering in sensor information systems (PEGASIS) [31], and the energy-efficient concentric clustering routing scheme (EECCRS) [32]. In these routing protocols, the network is clustered into groups according to the distribution of the system, there are several nodes in each cluster, and each node belongs to only one cluster. There is a cluster head (CH) in each cluster, and the CH needs to collect and process the data from the cluster members that are in the same cluster. The processed data are transmitted to the base node directly or indirectly. Hierarchical routing protocols have excellent expansibility and are easy to manage. However, forwarding data will cost tremendous energy. The other type of green routing protocol is flat routing, such as node spatial distribution (NSD) [33], geographic routing oriented sleep scheduling (GSS) [34], energy-balanced routing protocol (EBRP) [35], energy savings via opportunistic routing (ENS_OR) [36], and the energy-balanced routing method based on forward-aware factor (FAF-EBRM) [37]. Unlike hierarchical routing protocols, all nodes in flat routing protocols are the same, and each node communicates with the base node in a multihop manner. However, there are issues of poor extensibility and hole problems in flat routing.

The schemes mentioned above provide effective solutions for VNDN, but their applicability in VNDN with high mobility and high data volume is limited. Therefore, this article tries to fill this gap and proposes a blockchain-based key management and green routing scheme for VNDN, in which keys can achieve safe and efficient management and authentication by using blockchain. Additionally, it aims to decrease power consumption and delay.

3. Blockchain-Based Key Management

3.1. System Model. In this section, a blockchain-based key management scheme is introduced to solve the problem of lack of trust in interdomain nodes and to improve the authentication efficiency of key management. The system model of blockchain-based key management is shown in Figure 1, which contains the main parts described as follows.

3.1.1. Trusted Agency (TA). A trusted third-party authority that provides services for the domain is mainly used to generate public/private key pairs (PB_{Uk}, PV_{Uk}) for user i in the domain and public/private key pairs (PB_{Dk}, PV_{Dk}) for the domain. Meanwhile, the TA joins the consortium blockchain as a node of the blockchain to manage the generated keys securely and efficiently. Each TA is responsible for managing one domain.

3.1.2. Routing Node. VNDN routing nodes have relaying, caching, and broadcasting functions. The main function is to relay interest packets to nodes that have data and trace data packets back to consumers.

3.1.3. Domain. In an institution or organization, each domain contains multiple VNDN users and uses its private key to sign the users in the domain for authentication and to ensure the trustworthiness of the users. Each domain has a domain name that serves as a unique identifier in VNDN. The name of the domain can be expressed as follows:

$$|Public\,key|Hierarchy|PublicKeyHash|Version, \quad (1)$$

where *Public key* denotes the public key name of the domain, *Hierarchy* denotes the domain hierarchy to which the name belongs, *PublicKeyHash* is the hash of the domain public key, and *Version* denotes the version number.

3.1.4. User. A data requester or data producer consists of intelligent vehicles and terminal equipment in VNDN. The name of the user can be expressed as follows:

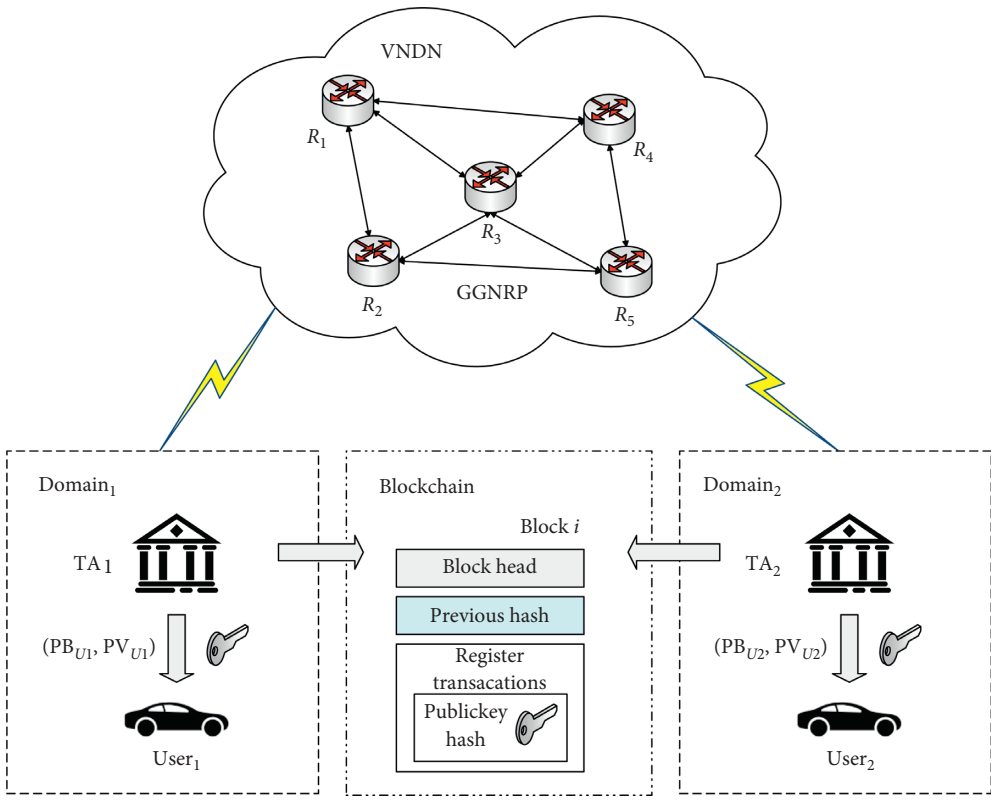

Figure 1: The system model.

$$|Global\ route|Hierarchy|PublicKeyHash|BlockLocation|TransactionHash|Version, \quad (2)$$

where *Global route* indicates the global and routable name for guiding the routing policy, *Hierarchy* denotes the user hierarchy to which the name belongs, *PublicKeyHash* indicates the hash of the user's public key, which will also be stored in the blockchain to verify the authenticity of the corresponding public key, *BlockLocation* indicates the location of the public key hash in the blockchain for fast retrieval, *TransactionHash* indicates the hash of the user's registered transaction, and *Version* indicates the version number.

Different from the existing schemes, the blockchain includes the block head and register transactions, the unique license, and the transaction record. As shown in Figure 1, each block contains a block header and a block body. The block header contains the hash value of the previous block, the timestamp, the hash value of the current block, and the root hash. The block body contains details of the transaction.

The proposed blockchain-based key management scheme has the following features.

(1) Integrity: all data are required to be signed by the data producer, and the data requester can easily verify the signature to be sure that the data have not been modified during the relaying process.

(2) Confidentiality: the content of any transaction message should be protected by asymmetric cryptography and digital signatures and should not be affected by any other entities.

(3) Reliability: after confirming that the data have not been modified, consumers can determine the source of the data so that they can trust the acquired data.

(4) Authentication: authentication services are the basis for achieving trustworthiness. After verifying that the received data have not been modified, the blockchain network and TA are used to verify the legitimacy of the data producer.

(5) Efficiency: the key retrieval and verification process is reduced to provide efficient key management and certification while providing basic services.

3.2. Key Management and Authentication. The blockchain-based key management design focuses on two main aspects: one is to verify the integrity of the data and the other is to quickly verify the credibility of the data packet. The producer uses the private key to sign the data packet and send it to the consumer. After the consumer receives the data packet, it first uses the producer's public key to verify the signature to ensure the integrity of the data. Then, it needs to authenticate the producer. If the data packet comes from a legitimate producer, the consumer trusts the data packet.

The designed blockchain-based key management scheme is divided into four main parts: system initialization, blockchain creation, packet transmission, and producer authentication.

Step 1: system initialization: system initialization is performed using an elliptic curve digital signature algorithm and asymmetric cryptography to ensure data confidentiality and integrity. TA_i first issues the public/private key pairs (PB_{Dk}, PV_{Dk}), (PB_{Uk}, PV_{Uk}) for the domain and user i within the domain.

Step 2: blockchain creation: user i creates a registration transaction and writes its public key hash to the transaction. The registered transaction is then sent to TA_i to verify its legitimacy and is added to the blockchain. TA_i verifies the legitimacy of the transaction, signs it, and broadcasts it to other blockchain nodes for consensus. The consensus nodes use the practical Byzantine fault tolerance (PBFT) consensus algorithm to conduct the consensus process on the transaction. After passing the consensus process, the registered transaction is uploaded to the consortium blockchain, and the public key hash of user i is stored in it. After that, TA_i returns the $BlockLocation_i$ and $TransactionHash_i$ to user i, who writes them into the name.

Step 3: packet transmission: the consumer sends an interest packet to the router to request the content it needs. If the data are cached in the local storage of the intermediate router, the router returns a data packet to the consumer. Otherwise, the router forwards the Interest packet to the producer. Finally, the data packet is sent back to the consumer by the producer in the same way. In the asymmetric cryptographic scheme, the decryption $\mathrm{Ver}_{\mathrm{PB}_k}(\cdot)$ of the digitally signed data using the public key of sender k is as follows:

$$\mathrm{Ver}_{\mathrm{PB}_k}\left(\mathrm{Sig}_{\mathrm{PV}_k}(H(m))\right) = H(m), \tag{3}$$

where $\mathrm{Sig}_{\mathrm{PV}_k}(\cdot)$ is the digital signature using the private key of sender k and $H(m)$ is the hash digest of message m.

Step 4: producer authentication: after the consumer receives the data packet, it uses the producer's public key to decrypt and verify the digital signature. However, only the public key from a legitimate producer can be trusted by the consumer. Therefore, the authenticity of the public key must be verified first. The consumer first checks the $BlockLocation_i$ and $TransactionHash_i$ fields in the name to quickly find the location of the registered transaction containing the hash of the public key. Then, the consumer obtains the public key hash stored in the blockchain from the "registration transaction" and calculates the obtained user's public key hash with the SHA-256 algorithm. After that, the two are compared and if the hash value is the same, the public key is proven to be true. Otherwise, the obtained public key is not the public key issued by a legitimate user.

4. Green Global Routing Scheme Based on the Node Relaying Pressure

4.1. Basic Definition. The symbols used in this paper are shown in Table 1.

Definition 1. (the maximal minimum hop)Assume that V is the set of nodes in VNDN and each node v_i's minimum hop is known as hop_i; then, the maximal minimum hop m is

$$m = \max\left(\mathrm{hop}_i\right), \quad v_i \in V. \tag{4}$$

Definition 2. (the node relaying pressure)If v_i's minimum hop is hop_i, m is the maximal minimum hop of the network and E_i is the residual energy of v_i, then v_i's relaying pressure press_i is

$$\mathrm{press}_i = \frac{2\left(m - \mathrm{hop}_i\right) + 1}{E_i}. \tag{5}$$

Definition 3. (the set of candidate relaying node)The set of neighbor of v_i is denoted as nbor_i, and v_i's minimum hop is hop_i; then, the set of v_i's candidate nodes cand_i is

$$\mathrm{cand}_i = \sum_{v_j \in \mathrm{nbor}_i} \mathrm{nbor}_i\left(\mathrm{hop}_j < \mathrm{hop}_i\right). \tag{6}$$

Considering that there are 18 nodes and one BS in VNDN shown in Figure 2, each node's minimum hop is known. In this network, hop_1, hop_2, hop_4, hop_{13}, and hop_{18} are all 3. Hop_3, hop_5, hop_8, hop_9, hop_{12}, hop_{14}, hop_{15}, and hop_{16} are 2. Hop_6, hop_7, hop_{10}, hop_{11}, hop_{17}, and hop_{19} are 1. According to the definitions, the maximal minimum hop m is 3. For node v_8, $\mathrm{hop}_8 = 2$, $m = 3$, we can obtain $\mathrm{press}_8 = 3/E_8$, and $\mathrm{nbor}_8 = \{v_4, v_7, v_{12}, v_{16}, v_{17}\}$, where hop_7, hop_{17} are less than 2; hence, we have $\mathrm{cand}_8 = \{v_7, v_{18}\}$.

An example of communications between nodes and a BS is shown in Figure 3, where the red dotted circle is the communication range of the nodes. To facilitate the analysis, we assume that all nodes in this model have the same maximal transmission radius r. The network is composed of n nodes and one BS. When their distance is larger than r, they are unable to send packets to each other directly. The tasks of the nodes are to collect data in their deployed areas and transmit the collected data to the BS. When a node has packets to send, it communicates with the BS in a multihop way. As shown in Figure 3, when v_1 has data to forward, the packet can reach the BS with the help of v_5 and v_6. In the initial phase, all nodes have the same energy, and the energy cost is related to the number of packets, the size of each packet, and the forwarding distance.

For the proposed GGNRP, the energy cost E_R of receiving k bits is

$$E_R = E_{\mathrm{elec}} * k, \tag{7}$$

where k is the size of the data packet and E_{elec} is the energy consumption that a node uses to send or receive one-bit data.

Table 1: Notations.

Symbol	Description
V	The set of sensor nodes in WSNs
r	The communication radius
m	The maximal minimum hop in network
E_T	The energy cost of transmission node
E_R	The energy cost of the receiving node
E_{elec}	The energy cost per bit
E_{amp}	The energy cost of signal amplification
hop_i	The minimum hop of v_i
nbor_i	The set of neighbors of v_i
cand_i	The set of candidate relaying nodes
p_{ij}	The path between node v_i and node v_j
cost_{ij}	The energy cost of p_{ij}
press_i	The relaying pressure of v_i
$\max_{ij}$	The maximal relaying pressure in p_{ij}

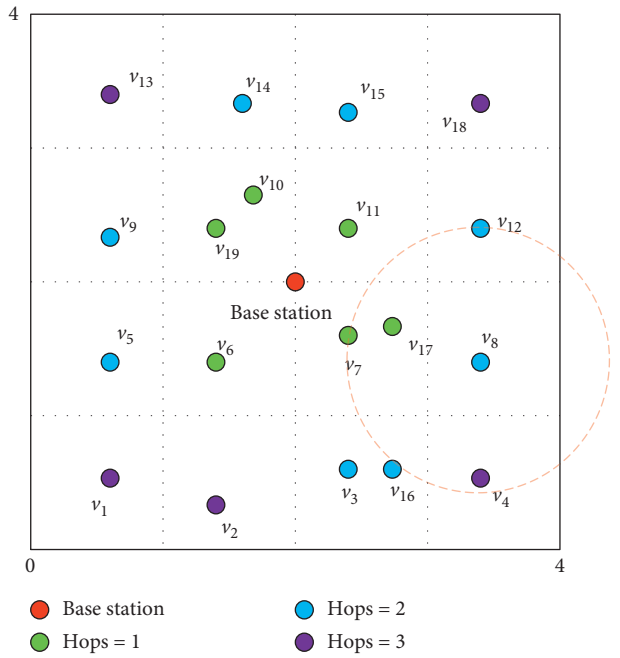

Figure 2: The minimum hop of each node.

The transmitting node also needs to consider the propagation loss, and the energy cost E_T of sending k bits to the receiving node is

$$E_T = E_{\text{elec}} * k + E_{\text{amp}} * k * d^{\beta}, \tag{8}$$

where E_{elec} represents the signal amplification cost, β is the wave loss factor, and d is the distance from the transmitting node to the receiving node.

4.2. GGNRP Process. The proposed GGNRP consists of two main phases: the routing establishment phase and the data forwarding phase. The flowchart of routing establishment is shown in Figure 4.

Each node obtains its neighbors by broadcasting, and then GGNRP calculates every node's minimum hop by broadcasting several times. Every node computes its

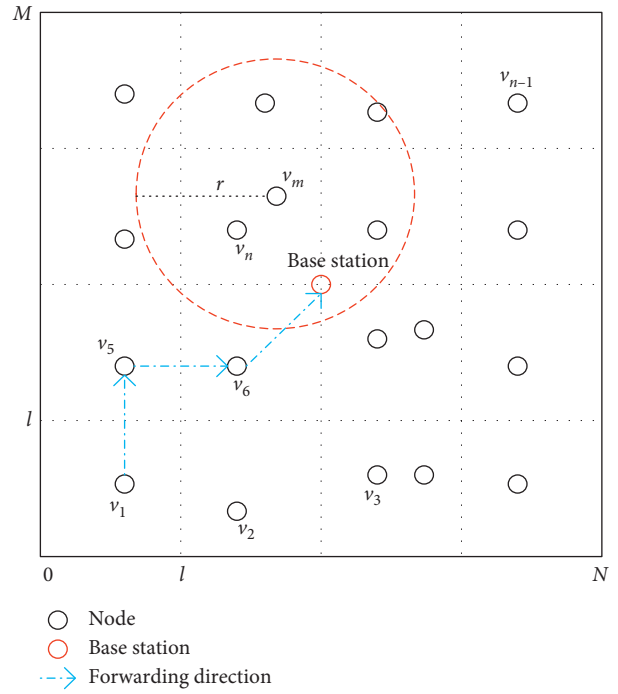

Figure 3: An example of communications between nodes and a BS.

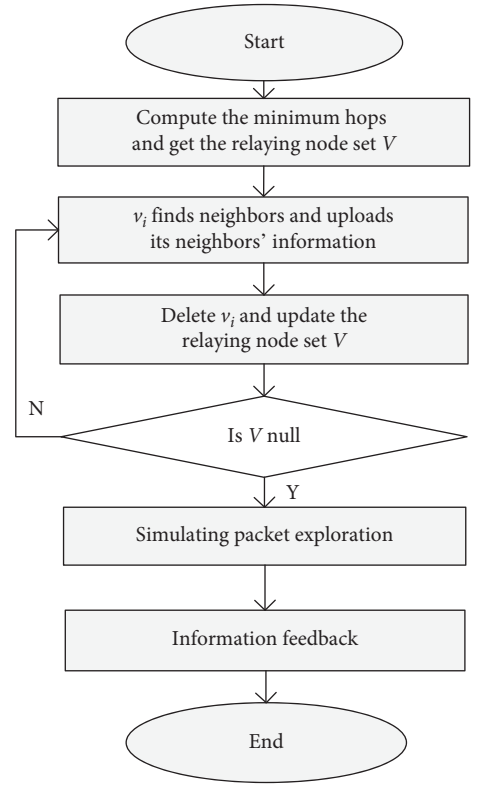

Figure 4: The flowchart of routing establishment.

candidate relaying nodes according to its neighbors' minimum hops and its minimum hops. After that, each node uploads its candidate relaying node set, the energy cost of the communication between itself and its candidate set, and its ID to the BS. Then, the BS simulates the process of nodes

sending exploring packets to the BS. The exploring packet that records its forwarding trace is transmitted only to the candidate relaying nodes of the nodes where the packet is. When the BS has computed all the nodes' shortest paths to itself, it will feed all path IDs and relevant information back to the related nodes. GGNRP avoids routing holes by limiting the forwarding objects in exploring data packets.

The routing establishment phase includes the following parts:

Step 1: calculating the minimum hop: GGNRP computes every node's minimum hop by broadcasting several times. Before this step, the minimum hops of the nodes in the network are all an unreachable number x. First, the BS broadcast packet has its maximum communication range, and the packet contains a number that is used to help the nodes compute their minimum hop, which is 1. If the number in the packet is less than its minimum hop, the node will change its minimum hop to this number. Then, the nodes whose minimum hops are equal to the number in the packet will broadcast new packets to their neighbors, and the number in the new packet is one larger than the old number. This process is repeated until there are no nodes whose minimum values are x.

As shown in Figure 5, v_6, v_7, v_{10}, v_{11}, v_{17}, and v_{19} are in the communication range of the BS. After BS broadcasting the messages, v_6, v_7, v_{10}, v_{11}, v_{17}, and v_{19} have the same minimum hop of 1. Then, v_6, v_7, v_{10}, v_{11}, v_{17}, and v_{19} begin to broadcast data. Similarly, v_3, v_5, v_8, v_9, v_{12}, v_{14}, v_{15}, and v_{16} set their minimum hop to 2. v_1, v_2, v_4, v_{13}, and v_{18} will achieve the same minimum hop of 3. According to Definition 3, we can obtain the candidate relaying nodes of each node in Figure 5 as shown in Table 2.

Step 2: simulating packet exploration: after Step 1, the BS has already collected enough information to finish the rest of the work in the routing establishment phase. GGNRP finds all the shortest paths to avoid additional energy consumption.

The format of the exploring packet is shown in Table 3, which contains the multicast objects and the forwarding trace. In the exploration process, the exploring packet always takes the candidate relaying nodes of the nodes that the packet is in as the multicast objects. When the exploring packet reaches a node, it will record its ID in its forwarding trace and update its multicast objects as the node. When the BS appears in the multicast objects of the packet, the packet will be transmitted to the BS directly.

The process of v_4's packet exploration is shown in Figure 6, where the subscript of the packet indicates the trace of the packet. Nodes v_3, v_8 and v_{16} are the candidate relaying nodes of v_4, so the packet$_4$ updates its content to $\{\{v_3, v_8, v_{16}\}, \{v_4\}\}$, and v_4 forwards it to v_3, v_8 and v_{16}. As packet$_{4\text{-}3}$ reaches v_3, it updates its content to $\{\{v_7\}, \{v_4, v_3\}\}$, and v_3 forwards it to v_7. The BS is the candidate relaying node of v_7, and packet$_{4\text{-}3\text{-}7}$ reaches the BS through v_7. Similarly, packet$_4$ is sent to v_8, packet$_{4\text{-}8}$ is forwarded to v_{17}, and packet$_{4\text{-}8\text{-}17}$ finally reaches the BS. Then, packet$_4$ is sent to v_{16}, packet$_{4\text{-}16}$ is forwarded to v_{17}, and packet$_{4\text{-}16\text{-}17}$ reaches the BS.

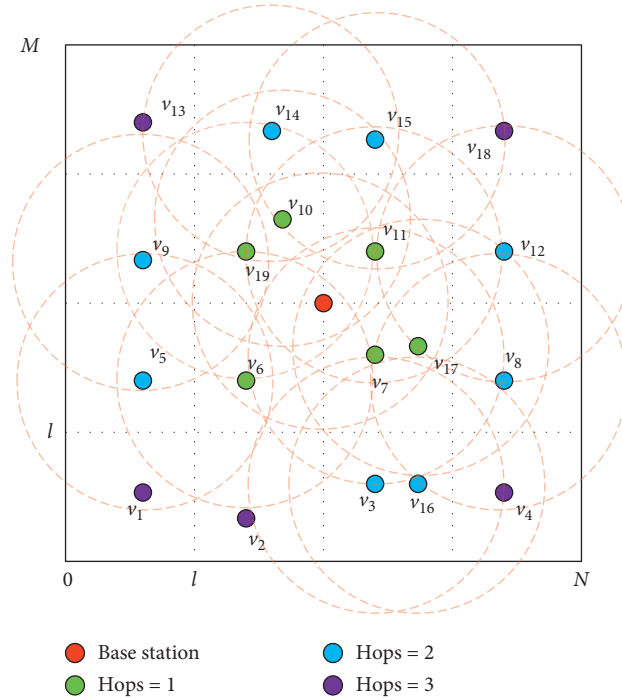

Figure 5: Compute the minimum hop.

Table 2: The candidate relaying nodes.

Node	The candidate relaying nodes
v_1	v_5
v_2	v_3
v_3	v_7
v_4	v_3, v_8, v_{16}
v_5	v_6
v_6	v_s
v_7	v_s
v_8	v_7, v_{17}
v_9	v_{19}
v_{10}	v_s
v_{11}	v_s
v_{12}	v_{11}, v_{17}
v_{13}	v_{14}
v_{14}	v_{10}, v_{19}
v_{15}	v_{10}, v_{11}
v_{16}	v_7, v_{17}
v_{17}	v_s
v_{18}	v_{12}, v_{15}
v_{19}	v_s

There are three shortest paths between v_4 and the BS, which are shown in Table 4.

Step 3: information feedback: the BS numbers all the paths that have only IDs. Then, the BS feeds the path IDs back to the related nodes. For example, as the BS obtains all the paths of v_4, it will feed information back

Table 3: The format of the exploring packet.

Multicast objects	Forwarding trace
$cand_i$	$\{v_0, \ldots, v_i\}$

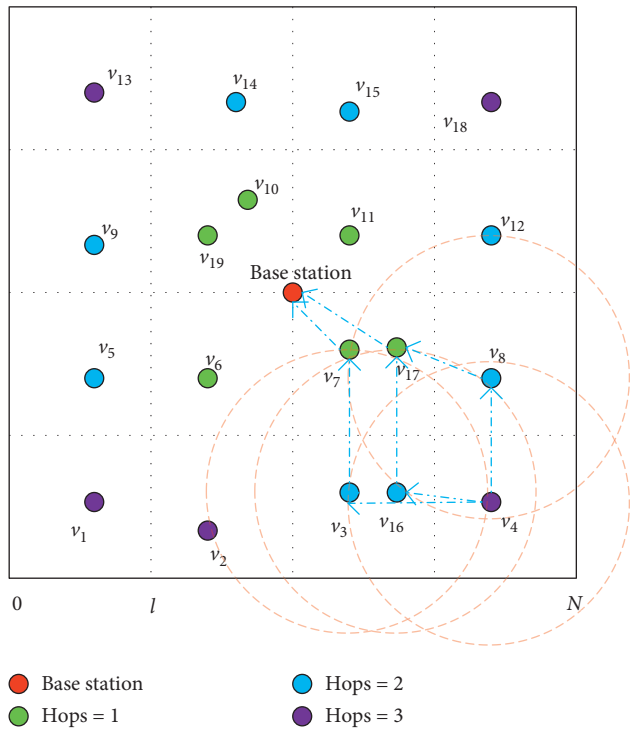

Figure 6: The process of v_4's packet exploration.

Table 4: The shortest path from v_4 to the BS.

Path ID	Path trace
p_{40}	$v_4 \longrightarrow v_3 \longrightarrow v_7 \longrightarrow$ BS
p_{41}	$v_4 \longrightarrow v_{16} \longrightarrow v_{17} \longrightarrow$ BS
p_{42}	$v_4 \longrightarrow v_8 \longrightarrow v_{17} \longrightarrow$ BS

to v_3, v_4, v_7, v_8, v_{11}, v_{12}, v_{16} and v_{17}; the information in each node is shown in Table 5.

In the data forwarding phase, when v_4 obtains p_{40} as the feedback path, it will check its local memory and find that v_3 is the next hop of v_4 in p_{40}, and v_4 sends the ready packets to v_3. Likewise, v_3 will find v_7 is the next hop; the packet will be sent to v_7. v_7 finds that BS exists in p_{40} so that the packet will be sent to the BS.

When the source node has data to send, it sends a request to the BS in the data forwarding phase. After receiving the request, the BS determines the optimal path according to the global energy information, the distribution of all nodes, and each node's relaying pressure. Then, the BS feeds the ID set of the path back to the source node. When there is more than one path ID in the set, the source node first checks whether the matched next hop exists with the last ID in the local memory; if it exists, the packet will be sent to the next hop. Otherwise, the node will check the previous ID in the set.

Table 5: The feedback information.

Node	The next hop and path ID
v_3	$v_7, \{p_{40}\}$
v_4	$v_3, \{p_{40}\}$ $v_{16}, \{p_{41}\}$
v_7	$BS, \{p_{40}\}$
v_8	$v_{17}, \{p_{42}\}$
v_{16}	$v_{17}, \{p_{41}\}$
v_{17}	BS, $\{p_{41}, p_{42}\}$

Specifically, the data forwarding phase includes two steps:

Step 1: global energy information cookie: the global energy information is important to decide the routing for the source node in GGNRP. The BS maintains the global energy information in GGNRP. The real-time energy information can be used to make the routing decision precisely. However, it will cause a great deal of energy consumption. GGNRP adopts the energy information cookie mechanism to avoid additional power consumption. When the source node starts to transmit data, the BS will compute every node's energy cost and update each node's energy information according to the number of packets, the size of each packet, and the distribution of the network.

Step 2: routing decision: the routing decision of GGNRP is made by the BS. The proposed routing decision algorithm is shown as Algorithm 1.

The BS determines the optimal routing according to the global energy information, the distribution of all nodes, and each node's relaying pressure. The lower the maximum relaying pressure of the path is and the less energy the path costs, the more likely the path is to be optimal. Since the multiple paths stored by each source node at the BS are the minimum number of hops, its performance in terms of delay is particularly excellent. However, the low-energy and high-burden nodes in the network cannot be well protected due to the limited paths. The BS will simulate the process of the nodes communicating with the BS. In the simulation, every time the packet reaches a node, the node will compare itself with its neighbors who have higher residual energy. If there are no nodes that have a higher weight than the current node, the packet will be sent to the original next hop. Otherwise, the packet will be sent to the node that has the highest weight and the BS will record the new path ID. This process repeats until the packet reaches the BS. Finally, the BS feeds the set of path IDs back to the source node. The packet is sent according to the path IDs set. When there is more than one ID in the set, the source node will check whether the next hop exists in the local memory in reverse order; if it exists, the packet will be sent to the next hop. Otherwise, the node will check the previous ID in the set in the memory.

GGNRP protects the lower-residual-energy nodes and higher-burden nodes by using the node relaying pressure as one of the routing decision factors. It reduces energy consumption by setting the path cost as one of the routing factors. In addition, all routing paths in GGNRP are almost the shortest

Input: Path_i
Output: S, w
(1) For $p_{ij} \in \text{Path}_i$
(2) For $v_k \in p_{ij}$
(3) If $\max_{ij} < \text{Press}_{v_k}$
(4) $\max_{ij} = \text{Press}_{v_k}$
(5) End If
(6) End For
(7) If $w < (1/(\max_{ij} * \text{cost}_{ij}))$
(8) $w = (1/(\max_{ij} * \text{cost}_{ij}))$
(9) $S = p_{ij}$
(10) End If
(11) End For
(12) Return S, w

Algorithm 1: Routing decision algorithm.

paths to the BS, which decrease the transmission delay and provide more transmission opportunities in VNDN.

5. Simulation Results

5.1. Simulation Setup. To validate the effectiveness of the proposed GGNRP, the performance of GGNRP is evaluated and compared with FAF-EBRM [37] in terms of energy consumption and delay. The power consumption and average delay of different schemes with a varying number of nodes are considered in different scenarios. The setup of simulation parameters is shown in Table 6.

5.2. Power Consumption and Average Delay. In this scenario, the monitoring area is set to $1000 \times 1000\ \text{m}^2$, and the number of nodes is set to 100. The lowest residual energy and average delay of GGNRP and FAF-EBRM are shown in Figures 7 and 8, respectively.

When the communication begins, the initial energy of all the nodes is 10 mJ. Before the 21st round, FAF-EBRM's lowest energy is slightly higher than that of GGNRP, which means that FAF-EBRM has a better performance than GGNRP in terms of energy consumption with low load. The reason is that FAF-EBRM chooses the high-energy-density forwarding area as the transmitting direction and GGNRP chooses the path cost and the node relaying pressure as the routing decision factors. In the 20th round, the energy of FAF-EBRM is 3 μJ higher than that of GGNRP. However, in the 21st round of transmission, the energy of GGNRP is 263 μJ higher than that of FAF-EBRM. Over time, the difference between GGNRP and FAF-EBRM increases. In the 57th round, the lowest residual energy of FAF-EBRM reaches 0 due to the first node, which consumes its energy, while GGNRP still has 1322 μJ of energy. These results illustrate that choosing the path cost and the node relaying pressure as the routing decision metrics has an advantage over choosing the high-energy-density forwarding area as the transmitting direction. This is because FAF-EBRM does not consider the total communication cost in the routing decision. GGNRP can support 66 rounds of communications, which indicates that GGNRP has 15.8% greater efficiency than FAF-EBRM.

As shown in Figure 8, in the first round, the average delays of FAF-EBRM and GGNRP are 34.1 ms and 14.4 ms, respectively, which means that the average delay of GGNRP is 57.8% lower than that of FAF-EBRM. From an overall perspective, the average delay of FAF-EBRM varies around 38.0 ms. While GGNRP maintains an average delay of 14 ms and has little delay variation. In the 24th communication round, the difference between FAF-EBRM and GGNRP reaches its maximum value, and the average delays of FAF-EBRM and GGNRP are 61.6 ms and 13.6 ms, respectively. The former is 4.53 times greater than the latter. In the 30th round of communication, the difference between FAF-EBRM and GGNRP reaches the minimum value, and the average delays of FAF-EBRM and GGNRP are 30.3 ms and 13 ms, respectively. The delay of FAF-EBRM is still 2.33 times that of GGNRP. For FAF-EBRM, nodes have the opportunity to be the next hop as long as their locations relative to the base station are closer than that of the source node. When the source node or the energy distribution is different, the delay of the network is different, which results in large delay variation in the network. In addition, FAF-EBRM prefers to the nodes in the energy density area as its next hop, which leads to packets being forwarded frequently among nodes and results in a higher delay than GGNRP. For GGNRP, the routing paths are optimized, GGNRP maintains its delay at a low level, and its delay variation is small.

5.3. Performance Comparisons at Different Scales. To evaluate the adaptability of GGNRP and FAF-EBRM at different scales, the power consumption and average delay results are shown in Figures 9 and 10, respectively, with varying numbers of nodes.

As shown in Figure 9, the remaining power is expressed as the number of forwarding packets. It is obvious that GGNRP can always afford more packets than FAF-EBRM, and the difference between them grows larger as the number of nodes increases. When the number of nodes is 150, the performance of GGNRP is almost the same as that of FAF-EBRM, and the numbers of forwarding packets of GGNRP and FAF-EBRM are 8044 and 7651, respectively. The performance of GGNRP is 5.13% higher than that of FAF-EBRM. When the number of nodes is 350, GGNRP can

Table 6: The simulation parameters setup.

Parameter	Value
The initial energy	10 mJ
The size of packet	1000 b
E_{amp}	10 pJ/b/m^2
E_{elec}	10 nJ/b
r	10 m

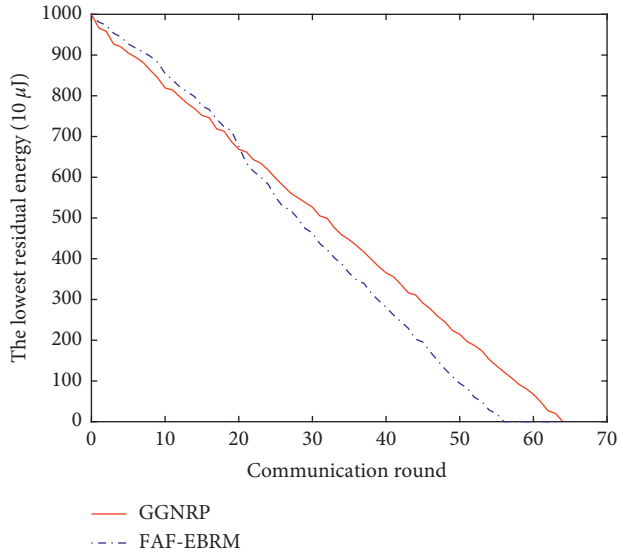

Figure 7: Power consumption of different schemes.

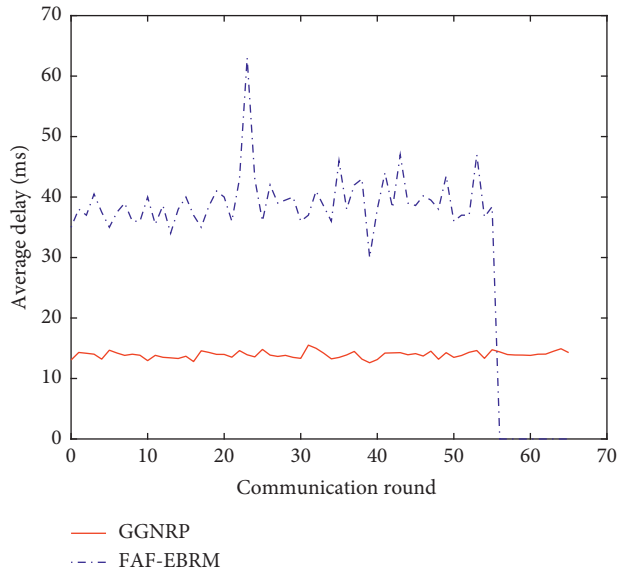

Figure 8: Average delay of different schemes.

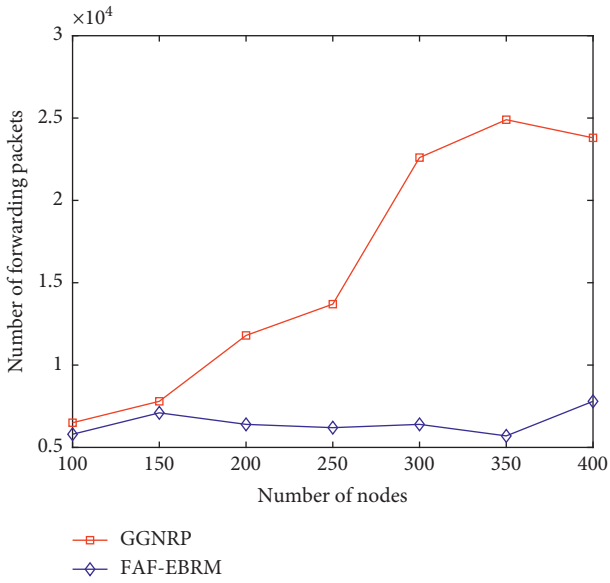

Figure 9: Power consumption of different schemes with varying number of nodes.

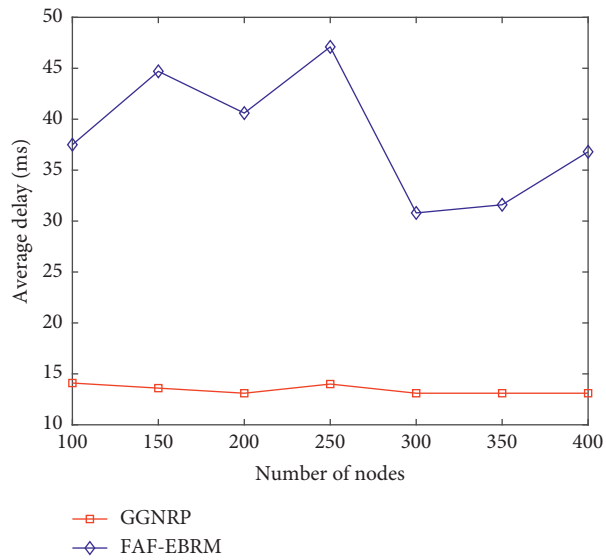

Figure 10: Average delay of different schemes with varying number of nodes.

afford 25032 packets, which is 4.37 times that of FAF-EBRM. These results show that GGNRP is more scalable than FAF-EBRM as the number of nodes varies. The power consumption of FAF-EBRM may even increase as the scale of WSNs grows. This occurs because a packet in FAF-EBRM needs to be transmitted to more nodes in the energy density area.

As shown in Figure 10, the average delay of GGNRP remains almost constant at approximately 13.7 ms, while the average delay of FAF-EBRM clearly varies. The average delay of FAF-EBRM is much larger than that of GGNRP. When the number of nodes is 100, the average delay of GGNRP is 13.98 ms, which is only 36.8% of that of FAF-EBRM. The results indicate that the proposed GGNRP decreases the average delay by 63.2%. When the number of nodes is 250, the average delays of GGNRP and FAF-EBRM are 13.934 ms and 46.1762 ms, respectively, and the difference between FAF-EBRM and GGNRP reaches the maximum value. When the number of nodes is 300, the average delays of GGNRP and FAF-EBRM are 13.13 ms and 29.91 ms, respectively, and the difference between FAF-EBRM and GGNRP reaches the maximum value. The results show that GGNRP is effective with varying scales.

5.4. Security Analysis. The security analysis of the proposed scheme is summarized as follows.

5.4.1. Distribution. Instead of setting a root key, the proposed key management scheme utilizes the distributed blockchain as a trust anchor to guarantee the authenticity of the keys by storing a hash value. The failure of a single node does not affect the key acquisition and verification, which avoids the failure of single point.

5.4.2. Trustworthiness. Blockchain solves the problem of cross-domain key authentication. In the absence of a root key, interdomain nodes cannot verify the legitimacy of the public key, which results in trust crisis. The proposed key management scheme stores the hash value of the public key in the blockchain and solves the trust problem of the public key by the tamper-evident nature of the blockchain.

6. Conclusion

In this article, a blockchain-based key management and green routing scheme is proposed for VNDN. A key management scheme is presented based on the blockchain by taking advantage of the distributed and antitampering characteristics of the blockchain. In this scheme, a flat hierarchical structure reduces the number of signatures and identity verifications needed to safely and efficiently verify the legitimacy of the producer. We elaborated on the mechanism of the scheme and the characteristics of its realization. To decrease the power consumption of nodes close to the BS and the transmission delay, the metric of node relay pressure is introduced, which makes the nodes with lower relay pressure more likely to be members of the selected forwarding path. The proposed GGNRP uses route exploration and feedback mechanisms in the routing establishment phase to avoid the coverage hole problem. In addition, GGNRP uses the node relay pressure and energy consumption as metrics in routing decisions, which reduces power consumption and transmission delays. The simulation results show that GGNRP can achieve better performance than FAF-EBRM in terms of power consumption and average delay.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. 61772562 and 62062019), the Key Project of Hubei Provincial Science and Technology Innovation Foundation of China (no. 2018ABB1485), and the Youth Elite Project of State Ethnic Affairs Commission of China (no. 2016-3-08).

References

[1] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: a distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020.

[2] L. Yao, A. Chen, J. Deng, J. Wang, and G. Wu, "A cooperative caching scheme based on mobility prediction in vehicular content centric networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5435–5444, 2018.

[3] C. Chen, J. Hu, T. Qiu, M. Atiquzzaman, and Z. Ren, "CVCG: cooperative V2V-aided transmission scheme based on coalitional game for popular content distribution in vehicular Ad-Hoc networks," *IEEE Transactions on Mobile Computing*, vol. 18, no. 12, pp. 2811–2828, 2019.

[4] L. Silva, N. Magaia, B. Sousa et al., "Computing paradigms in emerging vehicular environments: a review," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 3, pp. 491–511, 2021.

[5] C. Chen, C. Wang, T. Qiu, N. Lv, and Q. Pei, "A secure content sharing scheme based on blockchain in vehicular named data networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3278–3289, 2020.

[6] S. H. Ahmed, S. H. Bouk, D. Kim, D. B. Rawat, and H. Song, "Named data networking for software defined vehicular networks," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 60–66, 2017.

[7] T. Jin, X. Zhang, Y. Liu, and K. Lei, "BlockNDN: a bitcoin blockchain decentralized system over named data networking," in *Proceedings of the 2017 9th International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 75–80, Milan, Italy, 2017.

[8] J. Guo, M. Wang, B. Chen, S. Yu, H. Zhang, and Y. Zhang, "Enabling blockchain applications over named data networking," in *Proceedings of the 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, Shanghai, China, 2019.

[9] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1441–1454, 2015.

[10] D. B. Rawat, R. Doku, A. Adebayo, C. Bajracharya, and C. Kamhoua, "Blockchain enabled named data networking for secure vehicle-to-everything communications," *IEEE Network*, vol. 34, no. 5, pp. 185–189, 2020.

[11] J. Lou, Q. Zhang, Z. Qi, and K. Lei, "A blockchain-based key management scheme for named data networking," in *Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, pp. 141–146, Shenzhen, China, 2018.

[12] F. Ahmad, C. A. Kerrache, F. Kurugollu, and R. Hussain, "Realization of blockchain in named data networking-based internet-of-vehicles," *IT Professional*, vol. 21, no. 4, pp. 41–47, 2019.

[13] C. Chen, J. Li, V. Balasubramaniam, Y. Wu, Y. Zhang, and S. Wan, "Contention resolution in Wi-Fi 6-enabled internet of things based on deep learning," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5309–5320, 2021.

[14] C. Chen, B. Liu, S. Wan, P. Qiao, and Q. Pei, "An edge traffic flow detection scheme based on deep learning in an intelligent transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1840–1852, 2021.

[15] K. Harish, A. Harneet, and R. K. Singla, "Energy-aware fisheye routing (EA-FSR) algorithm for wireless mobile sensor networks," *Egyptian Informatics Journal*, vol. 14, no. 1, pp. 235–238, 2013.

[16] A. H. Sodhro, J. J. P. C. Rodrigues, S. Pirbhulal, N. Zahid, A. R. L. de Macedo, and V. H. C. de Albuquerque, "Link optimization in software defined IoV driven autonomous transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3511–3520, 2021.

[17] G. Sedky and A. E. Mougy, "BCXP: blockchain-centric network layer for efficient transaction and block exchange over name data networking," in *Proceedings of the 2018 IEEE 43rd Conference on Local Computer Networks (LCN)*, pp. 449–452, Chicago, IL, USA, 2018.

[18] C. Chen, Y. Zhang, Z. Wang, S. Wan, and Q. Pei, "Distributed computation offloading method based on deep reinforcement learning in ICV," *Applied Soft Computing*, vol. 103, Article ID 107108, 2021.

[19] J. Ma, T. Li, J. Cui, Z. Ying, and J. Cheng, "Attribute-based secure announcement sharing among vehicles using blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10873–10883, 2021.

[20] T. Chatterjee, S. Ruj, and S. D. Bit, "Security issues in named data networks," *Computer*, vol. 51, no. 1, pp. 66–75, 2018.

[21] T. Song, B. Cui, R. Li, J. Liu, and J. Shi, "Smart contract-based trusted content retrieval mechanism for NDN," *IEEE Access*, vol. 8, pp. 85813–85825, 2020.

[22] H.-K. Yang, H.-J. Cha, and Y.-J. Song, "Secure identifier management based on blockchain technology in NDN environment," *IEEE Access*, vol. 7, pp. 6262–6268, 2019.

[23] B. Li, M. Ma, and R. Xia, "Hierarchical identity-based security mechanism using blockchain in named data networking," in *Proceedings of the 2020 3rd International Conference on Hot Information-Centric Networking (HotICN)*, pp. 148–153, Hefei, China, 2020.

[24] G. Mauri, M. Gerla, F. Bruno, M. Cesana, and G. Verticale, "Optimal content prefetching in NDN vehicle-to-infrastructure scenario," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2513–2525, 2017.

[25] M. F. Majeed, S. H. Ahmed, and M. N. Dailey, "Enabling push-based critical data forwarding in vehicular named data networks," *IEEE Communications Letters*, vol. 21, no. 4, pp. 873–876, 2017.

[26] J. Cui, Y. Wang, J. Zhang, Y. Xu, and H. Zhong, "Full session key agreement scheme based on chaotic map in vehicular Ad-

Hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8914–8924, 2020.

[27] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular Ad-Hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.

[28] S. Hameed, S. A. Shah, Q. S. Saeed et al., "A scalable key and trust management solution for IoT sensors using SDN and blockchain technology," *IEEE Sensors Journal*, vol. 21, no. 6, pp. 8716–8733, 2021.

[29] W. Zheng, K. Wang, and F.-Y. Wang, "GAN-based key secret-sharing scheme in blockchain," *IEEE Transactions on Cybernetics*, vol. 51, no. 1, pp. 393–404, 2021.

[30] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Maui, HI, USA, 2000.

[31] S. Lindsey and C. S. Raghavendra, "PEGASIS: power-efficient gathering in sensor information systems," in *Proceedings of the 2002 IEEE Aerospace Conference*, Big Sky, MT, USA, 2002.

[32] M. Park, J. Choi, Y. Han, and T. Chung, "An energy efficient concentric clustering scheme in wireless sensor networks," in *Proceedings of the 5th International Joint Conference on INC, IMS and IDC*, pp. 58–61, Seoul, Republic of Korea, 2009.

[33] C. Li, L. Wang, T. Sun et al., "Topology analysis of wireless sensor networks based on nodes' spatial distribution," *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2454–2453, 2014.

[34] C. Zhu, L. T. Yang, L. Shu, J. J. P. C. Rodrigues, and T. Hara, "A geographic routing oriented sleep scheduling algorithm in duty-cycled sensor networks," in *Proceedings of the 2012 IEEE International Conference on Communications (ICC)*, pp. 5473–5477, Ottawa, Canada, June 2012.

[35] F. Ren, J. Zhang, T. He, C. Lin, and S. K. D. Ren, "EBRP: energy-balanced routing protocol for data gathering in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 12, pp. 2108–2125, 2011.

[36] J. Luo, J. Hu, D. Wu, and R. Li, "Opportunistic routing algorithm for relay node selection in wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 1, pp. 112–121, 2015.

[37] D. Zhang, G. Li, K. Zheng, X. Ming, and Z.-H. Pan, "An energy-balanced routing method based on forward-aware factor for wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 766–773, 2014.