IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received February 16, 2019, accepted February 26, 2019, date of publication March 4, 2019, date of current version March 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2902843

Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks

CHEN LYU[1], (Member, IEEE), XIAOMEI ZHANG[2], ZHIQIANG LIU[3], AND CHI-HUNG CHI[4]

[1]Department of Computer Science and Technology, Shanghai University of Finance and Economics, Shanghai 200433, China
[2]School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China
[3]Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[4]Data61, Commonwealth Scientific and Industrial Research Organization, Hobart, TAS 7005, Australia

Corresponding author: Xiaomei Zhang (xmzhang@sues.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61702319, Grant 61802252, and Grant 61672347, and in part by the Shanghai Sailing Program under Grant 17YF1405500.

ABSTRACT Wireless Sensor Networks (WSNs) have been widely used as the communication system in the Internet of Things (IoT). In addition to the services provided by WSNs, many IoT-based applications require reliable data delivery over unstable wireless links. To guarantee reliable data delivery, existing works exploit geographic opportunistic routing with multiple candidate forwarders in WSNs. However, these approaches suffer from serious Denial of Service (DoS) attacks, where a large number of invalid data are deliberately delivered to receivers to disrupt the normal operations of WSNs. In this paper, we propose a selective authentication-based geographic opportunistic routing (SelGOR) to defend against the DoS attacks, meeting the requirements of authenticity and reliability in WSNs. By analyzing statistic state information (SSI) of wireless links, SelGOR leverages an SSI-based trust model to improve the efficiency of data delivery. Unlike previous opportunistic routing protocols, SelGOR ensures data integrity by developing an entropy-based selective authentication algorithm, and is able to isolate DoS attackers and reduce the computational cost. Specifically, we design a distributed cooperative verification scheme to accelerate the isolation of attackers. This scheme also makes SelGOR avoid duplicate data transmission and redundant signature verification resulting from opportunistic routing. The extensive simulations show that SelGOR provides reliable and authentic data delivery, while it only consumes 50% of the computational cost compared to other related solutions.

INDEX TERMS Internet of Things, opportunistic routing, DoS attacks, selective authentication.

I. INTRODUCTION

Wireless sensor networks (WSNs) have been developed in the Internet of Things (IoT) and play an important role to provide a wide range of applications through sensors, such as smart home, traffic management, smart grids and environment monitoring [1], [2]. A wireless sensor network contains some receivers/sinks and a number of distributed sensor nodes which collaboratively collect and transmit data to perform a variety of missions. Built upon WSNs, providing reliable data delivery is usually expected for IoT-based applications. One example of such applications is smart healthcare, which is used for the purpose of monitoring, tracking or treating patients [3]. In this application, sensor nodes collect the patient's physical data and then deliver them to the doctor. Based on the collected data, the doctor is aware of the physiological status of the patient, and is able to make a suitable diagnosis.

The above application requires WSNs to provide reliable data delivery, which is regarded as the critical factor for the success of diagnosis. However, based on the varying and shared wireless mediums, WSNs are susceptible to link

The associate editor coordinating the review of this manuscript and approving it for publication was Weizhi Meng.

failures due to signal interference or signal fading, which may significantly decrease the quality of service [4], [5]. Therefore, supporting reliable data delivery becomes a challenging problem in WSNs. To address this issue, many multi-path routing strategies [6]–[8] have been proposed to improve the reliability of data delivery in WSNs. However, maintaining a multi-path route for a data flow has a high communication cost for the instability of wireless channels. Moreover, since data packets are transmitted over multiple paths to receivers, more transmission contentions and signal interferences are introduced leading to additional transmission failures in the network.

Recently, an efficient approach to meet the requirement of data reliability is exploiting (geographic) opportunistic routing which does not determine the routing path before data transmission [9]–[12]. With the broadcast and shared nature of the wireless channel, it allows packet transmission to be overheard by multiple sensor nodes. Instead of one singer forwarder in traditional routing, multiple candidate forwarders are selected in the opportunistic routing, which are ordered based on the priorities defined by the sender of the packet. Therefore, the packet transmission is not disrupted as long as one candidate in the forwarder set successfully relays it. Compared with multi-path routing, opportunistic routing has better performance because no additional transmission contentions or signal interferences exist between candidates.

As one of the traditional routing protocols, geographic routing is an attractive choice with regard to dynamic wireless links, since it does not need to establish and maintain paths from source nodes to sinks [13]. Therefore, the combination of geographic routing and opportunistic routing has been referred to as geographic opportunistic routing [14]–[16]. Existing geographic opportunistic routing approaches can achieve high reliability over wireless links (e.g., [16]). However, they suffer from serious Denial of Service (DoS) attacks. Malicious attackers may deliberately send a large number of invalid data with illegitimate signatures to sinks, aiming to waste the network resources and disrupt the normal operations of WSNs [17]. In particular, opportunistic routing aggravates DoS attacks that invalid data can be reliably delivered to receivers with multiple candidate forwarders, which will be validated by our theoretical analysis and experiment results in the latter part of this paper. To defend against such attacks, we need a security authentication scheme, which can guarantee that data packets are sent from legitimate sensor nodes, and they are not sourced or modified by attackers during transmissions. However, this opens plenty of new issues.

First, involving an existing digital signature scheme for authentication may tremendously increase the computational cost of a sensor node and extend the delay of data delivery. Sensor nodes are typically computational and energy constrained. Prior work has shown that verifying one ECDSA signature needs about 1.62 seconds on MICA2 and MICAz motes [18]. Verifying the digital signature of every incoming data packet on a sensor node would fast exhaust its resource. Therefore, a new lightweight authentication mechanism to isolate DoS attackers is mandatory for WSNs. Second, verification of data packets may break down the priorities of candidate forwarders defined by the opportunistic routing, since the verification delay is generally much greater than the transmission time of data packets. Hence, restoring the priorities of candidate forwarders to achieve the integrity and reliability of data should be our main design goal. Third, duplicate transmission of invalid data or redundant verification may be incurred by the opportunistic routing. For example, if the first candidate drops one invalid packet after the process of verification, the second candidate cannot certain whether the data packet is dropped for being invalid or link failure. It may skip the process of verification and then proceed to deliver the invalid data packet. Alternatively, it may perform the same process of verification and then drop it. Therefore, a scheme of sharing the verification information between candidates should be designed to minimize the incurred overhead.

In this paper, we propose a selective authentication based geographic opportunistic routing (SelGOR) to defend against the DoS attacks in WSNs. SelGOR aims at ensuring the authenticity and reliability of data packets for IoT-based applications. To improve the efficiency of data delivery, SelGOR analyzes statistic state information (SSI) of wireless links, and builds an SSI-based trust model for the construction of a trust-based geographic opportunistic routing. In addition, in contrast to existing opportunistic routing, SelGOR leverages an entropy-based selective authentication algorithm to ensure data integrity. Our selection authentication algorithm is performed based on the signatures with high entropy (unknown state) or low entropy (certain state), and is able to reduce the computational cost of the sensor node. Especially, we design a cooperative verification scheme to combine the opportunistic routing with selective authentication algorithm, which includes "verification notice" and "warning push." The mechanism of verification notice is utilized to restore the priorities of candidate forwarders in opportunistic routing. The mechanism of warning push is employed to share the verification information of invalid signatures between candidates, which could also accelerate the isolation of attackers. According to warning push, candidate forwarders are allowed to cancel duplicate data transmission or redundant signature verification. The extensive comparative evaluation shows that Our SelGOR could block 80% of invalid data with a low communication overhead, while it saves 50% of computational resources and 50%-70% of bandwidth resources compared to other schemes.

To the best of our knowledge, our work is the first attempt for an efficient and reliable data delivery protocol while explicitly maintains the desired authentic data in WSNs. The main contributions of this work are summarized as follows:

- We design an SSI-based trust model which is exploited as the basis of constructing a trust-based geographic opportunistic routing to improve the reliability of data delivery.

- We identify the DoS attacks pose serious security threats to the opportunistic routing in WSNs. Subsequently, an entropy-based selective authentication algorithm is introduced to isolate the DoS attackers with low computational cost.
- A distributed cooperative verification scheme is exclusively proposed to cooperate the selective authentication algorithm with the opportunistic routing, while it also significantly reduces the number of transmission of invalid data and the number of signature verification incurred by the opportunistic routing.
- Theoretical analysis and empirical validations are done to show our SelGOR effectively defends against the DoS attacks. It is fairly reliable even over unstable wireless links, and low-cost in terms of computational and communication resources.

The rest of this paper is organized as follows. Section II describes the related work. Section III discusses our network and security model. The protocol SelGOR is presented in Section IV. The effectiveness analysis of SelGOR against DoS attacks is shown in Section V. The performance evaluation is provided in Section VI. At last, we conclude our paper and outline the future work in Section VII.

II. RELATED WORK

There have been many researches on opportunistic routing exploiting the spatial diversity of wireless transmissions for data delivery in wireless ad hoc networks [9]–[12], [19]–[21]. As one branch of opportunistic routing, geographic opportunistic routing which makes use of the geographic location to choose the candidate forwarders in the neighbor list is also widely studied in the literature [14]–[16], [22].

Sanchez-Iborra and Cano [10] propose the opportunistic routing named JOKER in order to balance the tradeoff between multi-media service and energy consumption for mobile devices. Their JOKER uses the routing metric combining the reliability of wireless links with the distances to receivers for candidate selection. To minimize the energy consumption and maximize the lifetime of WSNs, Luo *et al.* [11] optimize the candidate forwarder set based on the distances to receivers and the remaining energies of sensor nodes, and then use opportunistic routing for data delivery in the model of one-dimensional queue network. So and Byun [12] design an opportunistic routing for load balance in the duty-cycled wireless sensor networks. In their scheme, the number of candidate forwarders is controlled based on the estimation of forwarder cost in order to reduce redundant data forwarding caused by the opportunistic routing. Zeng *et al.* [14] propose a geographic opportunistic routing in the multi-rate wireless networks. They study the strategies of candidate selection and candidate coordination, and then design an effective metric for the opportunistic routing to achieve high network throughput. Cheng *et al.* [16] address the problem of Quality of Service (QoS) provisioning with the constraints of reliability and end-to-end delay in WSNs. They formulate it as an optimization problem, and then design an efficient geographic opportunistic routing to provide QoS with low communication cost.

Although these works are on the basis of opportunistic routing, they mostly address the issues of QoS, load balance or energy efficiency. In terms of security, Salehi and Boukerche [23] address black hole attacks on opportunistic routing in the wireless mesh networks, where nodes deliberately drop the data packet that they are supposed to transmit. To defend against such attacks, they make use of Markov chain to establish a packet salvaging model for the opportunistic routing. Zhang *et al.* [24] propose a framework for the opportunistic routing to provide both privacy preserving and security protection for delay/disruption-tolerant networks. The security and privacy are realized according to anonymous routing, the confidentiality of the routing metric and key agreement for data communication. SGOR [25] is a geographic opportunistic routing which is proposed to cope with a wide of attacks in WSNs. Thus, a location verification algorithm is designed on received signal strength [26] to address the location spoofing attack. To response to black hole attacks in the routing, SGOR utilizes an ambient-sensitive trust model to construct the routing metric for the opportunistic routing. These discussed solutions provide a range of improvements to the security of the opportunistic routing. However, none of them could defend against any DoS attacks, which pose serious threats to the opportunistic routing over wireless links.

As to the DoS attacks, many security mechanisms have been investigated in the field of Internet [27], Vehicular Ad Hoc Networks [28], Cyber-Physical Systems [29], cloud computing [30] and Wireless Sensor Networks [18], [31]–[34]. Due to the different objectives of attackers, there are a variety of DoS attacks in WSNs. Ning *et al.* [18] address the DoS attacks with respect to broadcast authentication. They propose a weak authentication scheme by exploiting the mechanism of message-specific puzzles to mitigate the DoS attacks on both digital signature schemes and TESLA-based broadcast authentication scheme [35] in WSNs. The limitation of this scheme is that it requires relatively high computational cost for the packet sender. Moreover, the end-to-end delay of data packets is largely extended for solving the puzzles. To isolate the DoS attackers, Agah and Das [31] divide the DoS attacks into passive attacks and active attacks, and then exploit game theory to categorize nodes according to their behaviors. However, their scheme requires a centralized base station to monitor the behaviors of all the sensor nodes. Deng *et al.* [32] address the path-based DoS attacks, and propose a scheme based on one-way hash chains to defend against such attacks. However, since the routing paths need to be determined before data transmission, their solution cannot apply to the opportunistic routing. In WSNs, there are some other secure schemes [33], [34] proposed to resist the DoS attacks on code dissemination protocols, which spread a new program image to all of the sensor nodes. Nevertheless, all the above schemes do not deal with the DoS attacks on the opportunistic routing. In this work, we attempt to address this issue, and introduce the selective authentication algorithm with low computational cost to isolate the DoS attackers in WSNs. In order to efficiently combine the selective authentication algorithm with the geographic opportunistic routing, we design a distributed cooperative verification scheme by minimizing the negative impact caused by the opportunistic routing. In addition, our work is the first to identify the opportunistic routing aggravates the impact of DoS attacks on data delivery based on theoretical analysis and evaluation results.

III. NETWORK AND SECURITY MODEL

A. NETWORK MODEL

We assume a multi-hop WSN which consists of a number of sensor nodes and some sinks/receivers is deployed for one application of IoT. Sensor nodes within the wireless transmission range R could directly send data to each other. The multi-hop communication is enabled when their Euclidian distance is greater than the transmission range. We assume that the sensor network is a dense network, where each sensor node has plenty of neighbor nodes. Thus, this network can be defined by a graph $G(V, L)$, where V depicts the set of sensor nodes and L depicts the set of direct links between sensor nodes. We denote a link $l_{i,j} \in L$ if the Euclidian distance between the sender nodes $i \in V$ and the receiver node $j \in V$ is less than the wireless transmission range R.

We assume sensor nodes are stationary, and know their location information and the position information of sinks. Besides, nodes are aware of the location information of their neighbor nodes through beacon messages in the general geographic routing, i.e., a sensor node periodically broadcasts its identity, location information and residual energy in beacon messages [13]. As the energy issue is a major challenge in the WSN, we assume that sinks are equipped with powerful devices and other sensor nodes operate on limited batteries. Based on beacon messages, it is feasible for nodes to obtain the energy information of their neighbor nodes.

In this work, we mainly concentrate on the performance of data delivery in the network layer. To achieve the coordination of candidate forwarders in our protocol, we exploit a modified MAC protocol which is proposed for opportunistic routing based on RTS/CTS/ACK mechanism in the IEEE 802.11b [15]. However, other MAC layer problems such as hidden terminal or collision avoidance are not considered in this paper.

For security protection, a Public Key Infrastructure (PKI) is required for key management in the WSN [36]. We assume each sensor node has a pair of ECDSA keys: a public key for verification and a private key for signing data packets. A trusted Certificate Authority (CA) would endorse the public keys as legal identities of sensor nodes. In the real deployment, sink nodes or developers of applications could act as the role of CA. We assume each sensor node knows the public keys of all nodes, and never releases its private key to another party.

B. SECURITY MODEL

In this paper, our goal is to design an efficient and reliable data delivery protocol which technically maintains the desired authentic data in WSNs. Therefore, we should provide these important properties for data packets.

1) DATA INTEGRITY

Before transmitting a data packet, a sensor node is supposed to ensure the authenticity of data relayed by its neighbor nodes. Otherwise, sinks would receive plenty of invalid data from the DoS attackers, which disrupts the normal operations of applications. To provide the property of data integrity, an authentication scheme is indispensable for WSNs.

2) NON-REPUDIATION

The property of non-repudiation usually involves authentication. It permits a sink to prove to third parties that the sender node is responsible for the data packet. According to this property, sinks can ascertain the sender of any invalid data packet and report attackers to trusted CAs.

3) DATA RELIABILITY

Because of the broadcast and shared nature of the wireless medium, data packets are susceptible to lose for link failures. Even the effect of data loss is inevitable in WSNs, it should not disable the operations of applications based on IoT. Therefore, it is essential to guarantee high reliability for any data delivery protocol.

4) DOS ATTACKS RESISTANT

Without any authentication scheme, the DoS attackers may send a lot of invalid data packets in the network to waste communication resources of networks or disrupt the normal data delivery. Moreover, sensor nodes normally have limited computational and energy resources. To defend against DoS attackers, the authentication scheme should have low computational cost for energy efficiency in WSNs.

We consider each sensor node registers with the CA by preloading a public/private key pairs: PK and SK. The private key SK_i is exploited by the sender node i to sign the data packet. A receiver node/sink can ensure the authenticity of the data packet by the public key PK_i of the sender. We consider DoS attacks are caused by one or more attackers sending a number of illegitimate signature packets to sinks. To avoid being detected, attackers may sometimes send valid data with legitimate signatures in the network. If someone reports the DoS attackers to the CA or any trusted legal authority, they will seek to repudiate data packets that have been created by them. In this work, we do not consider the location spoofing attacks and black hole attacks, which can be addressed by the existing security schemes [23], [25]. The issues of eavesdropping and data privacy are out of the scope of this paper.

IV. SELECTIVE AUTHENTICATION BASED GEOGRAPHIC OPPORTUNISTIC ROUTING

In this section, we first give an overview of our selective authentication based geographic opportunistic routing, and then describe its primary components.

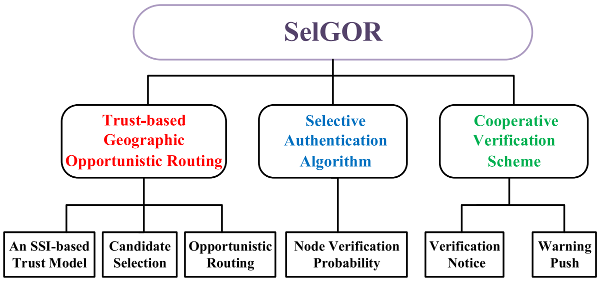

SelGOR
Trust-based Geographic Opportunistic Routing
Selective Authentication Algorithm
Cooperative Verification Scheme
An SSI-based Trust Model
Candidate Selection
Opportunistic Routing
Node Verification Probability
Verification Notice
Warning Push

FIGURE 1. The overview of SelGOR.

A. PROTOCOL OVERVIEW

Our SelGOR protocol mainly contains three major components: trust-based geographic opportunistic routing, selective authentication algorithm and cooperative verification scheme. As shown in Figure 1, we first give the overview of the three components as follows:

- Trust-based geographic opportunistic routing: By collecting and analyzing historical data transmission of wireless links, a sensor node establishes an SSI-based trust model and dynamically updates it in WSNs. When a data packet arrives at a sensor node, the sensor node needs to determine the candidate forwarder set from its neighbors in order to achieve reliable data delivery in opportunistic routing. To do so, the sensor node assigns the priority to each candidate forwarder based on the routing metric, which is defined on the SSI-based trust model. Therefore, trust-based geographic opportunistic routing includes an SSI-based trust model, candidate selection and opportunistic routing. We will present its construction in Section IV-B.
- Selective authentication algorithm: Before sending any data packet, a sensor node needs to ensure the authenticity of the packet to defend against DoS attacks. We present an entropy-based selective authentication algorithm that can quickly block the invalid data packets without checking all signatures on every hop. If the sensor node knows more/less information about a received signature, it could be checked with a lower/higher probability. In addition, we leverage node verification probability, which could be actively adjusted based on the received invalid signatures, to achieve isolation of attackers. We will present this algorithm in Section IV-C.
- Cooperative verification scheme: When a sensor node begins to verify a data packet before transmission, it undermines the priorities of candidate forwarders defined by the opportunistic routing. Hence, we design the mechanism of verification notice to address this issue. After verification, we could exploit the mechanism of warning push to share the verification result between candidate forwarders for efficient and fast isolation. Cooperative verification scheme, including the mechanism of verification notice and warning push, is present in Section IV-D.

In SelGOR, a data packet M is opportunistically routed from the source to the sink. As illustrated in Figure 2, each route segment consists of a set of candidate forwarders (e.g., node R_1, R_2 and R_3). Our SelGOR works as follows.

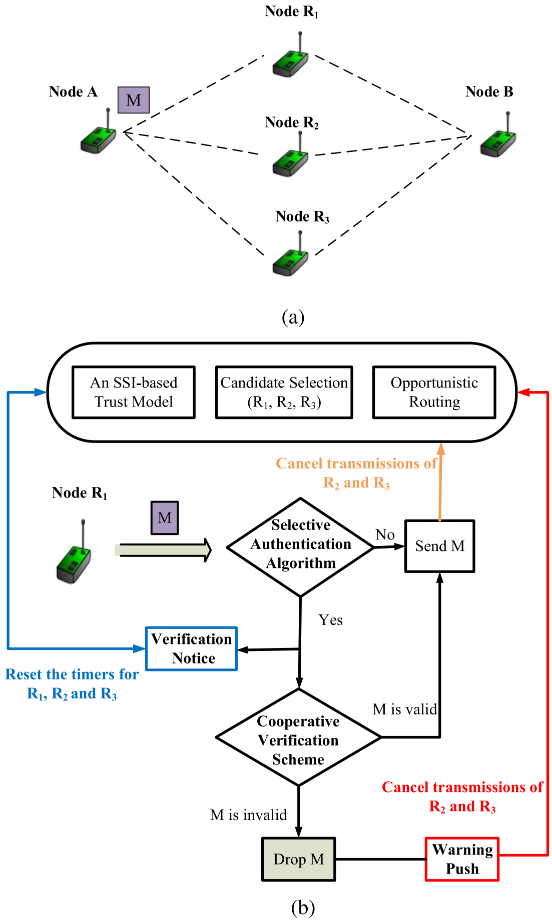

Node R_1
Node A
M
Node B
Node R_2
Node R_3
(a)
An SSI-based Trust Model
Candidate Selection (R_1, R_2, R_3)
Opportunistic Routing
Cancel transmissions of R_2 and R_3
Node R_1
M
Selective Authentication Algorithm
No
Send M
Yes
Verification Notice
Reset the timers for R_1, R_2 and R_3
M is valid
Cooperative Verification Scheme
Cancel transmissions of R_2 and R_3
M is invalid
Drop M
Warning Push
(b)

FIGURE 2. The illustration of SelGOR. (a) The network topology. (b) The work flow of node R_1.

When M arrives at node A, the relay node A would determine the priorities of candidate nodes based on the routing metric, which is constructed based on the SSI-based trust model. In our example, we assume that the decided order is $\{R_1, R_2, R_3\}$, which indicates nodes would forward M with the priority rule ($R_1 > R_2 > R_3$). The priority rule is usually realized by the distinctive timer run on each candidate node [10], [15]. Accordingly, node R_1 becomes the first candidate node to relay the data packet. If the link quality is poor, it cannot receive M and the transmission is interrupted. However, due to the shared wireless channel, node A and other candidate nodes do not hear any packet transmission from node R_1 at this moment, and then detect the failure of the wireless link. Node A adjusts the trust of link l_{A,R_1} in the SSI-based trust model. Meanwhile, node R_2 is activated to transmit M. When its timer expires, node R_2 becomes the relay node of M with the principle of opportunistic routing.

Providing that node R_1 receives the packet M correctly, it performs selective authentication algorithm to decide to check M or not. If it skips the verification process based on the node verification probability of node A, the data packet is promptly transmitted to the next relay node. Based on the scheme of opportunistic routing, node R_2 and R_3 cancel the transmissions of M by disabling their own timers. However, if it decides to verify M, a packet of verification notice should be multicast to the other candidates with low priorities in order to reset their timers. After finishing verification, node R_1 sends out M to the next relay node if it is valid. Concurrently, node R_2 and R_3 disable their timers to cancel the transmissions of M. In case M does not pass the verification, node R_1 drops M and increases the node verification probability of node A. To share the verification result, a packet of warning push is then sent to the other candidates with low priorities. Once receiving the warning push, node R_2 and R_3 cancel the transmissions of M and simultaneously increase the node verification probability of node A.

It is possible to consider that node R_1 would deliberately drop M and send warning push after successful verification of M. In this work, we do not exclusively deal with this issue to simplify our model. However, this attack is likely to be addressed by designing a new reputation model for sensor nodes.

B. TRUST-BASED GEOGRAPHIC OPPORTUNISTIC ROUTING

Our trust-based geographic opportunistic routing consists of an SSI-based trust model, candidate selection and opportunistic routing to provide reliable data delivery. First, we design an SSI-based trust model by characterizing unreliable wireless links in WSNs. Second, we integrate the SSI-based trust model into our routing metric to select multiple candidates from neighbor nodes. At last, we describe the scheme of opportunistic routing.

1) SSI-BASED TRUST MODEL

By collecting and analyzing historical data transmission of neighbors, we exploit the ratio of the number of packets successfully delivered to the number of packets sent to characterize the trust of a link. At a high level, a sensor node k divides the timeline into a chain of observation intervals, which has the same length of n. During each observation interval, it is possible for node k to hear the wireless channel and check whether a data packet is truly forwarded by the selected neighbor node. For one of the observation intervals, the number of data packets transmitted by a neighbor node i is denoted as $NS_k^i(n)$, and the number of data packets sent to it is denoted as $ND_k^i(n)$. Therefore, node k could evaluate the trust of the link $l_{k,i}$, which is defined as $T_k^i(n)$ $(0 \leq T_k^i(n) \leq 1)$.

$$T_k^i(n) = \frac{NS_k^i(n)}{ND_k^i(n)}. \tag{1}$$

At the start of an observation interval, $NS_k^i(n)$ is initialized to zero and $ND_k^i(n)$ is initialized to one. When a data packet is relayed by node k to node i as the next hop node, $ND_k^i(n)$ is updated by $\alpha ND_k^i(n) + 1$, where α $(0 < \alpha \leq 1)$ is the parameter of adjustment rate in the system. Once node k hears a successful transmission by node i, $NS_k^i(n)$ turns into $\alpha NS_k^i(n) + 1$ so that the trust of the link $l_{k,i}$ is positively changed. Otherwise, $NS_k^i(n)$ becomes $\alpha NS_k^i(n)$ in terms of a failed transmission, and the trust degree is negatively changed.

In order to achieve the stability of the trust for candidate selection in opportunistic routing, the trust of link $l_{k,i}$ at time t is updated through iterations in node k's neighbor list:

$$T_k^i(t) = \omega T_k^i(t-n) + (1-\omega) T_k^i(n), \tag{2}$$

where ω $(0 \leq \omega \leq 1)$ is the weight to balance the preference between current and historic state information. As there is no ambiguity with respect to the time, we use T_k^i for brevity.

2) CANDIDATE SELECTION

In opportunistic routing, plenty of routing metrics have been developed in the literature to select candidates for load balance, energy saving or QoS provisioning in WSNs. By jointly considering the proposed techniques and unreliable wireless links, we mainly exploit three factors to design our routing metric, including the single-hop distance progress [14], [16], the trust degree and the remaining energy of the neighbor node.

Supposing that a node k is sending a data packet to the sink/receiver (denoted as s), and node i is one of its neighbor node which is set closer to the sink than node k. When a data packet is transmitted from node k to node i, we define single-hop distance progress as SP_k^i:

$$SP_k^i = D(k,s) - D(i,s), \tag{3}$$

where $D(k,s)$ is the Euclidian distance between node k and node s. We define Q_k as the available candidate forwarder set for node k, where all nodes have positive single-hop distance progresses.

In the traditional geographic routing, node k selects a single candidate with the highest SP_k^i in Q_k for data delivery. However, more thought must be given to improving data delivery. On the one hand, we should integrate the trust degree of the wireless link in our routing metric. Based on the SSI-based trust model, node k is able to obtain the trust T_k^i of link $l_{k,i}$ in the neighbor list. Inspired by the prior research [16], we take T_k^i times SP_k^i in our routing metric to improve the QoS of data delivery. On the other hand, some links may become expired due to energy shortage of sensor nodes. Hence, the remaining energy (denoted as RE) should be also taken into account. In the WSN, node k is aware of the remaining energy RE^i of node i according to the scheme of periodic beacon messages in the geographic routing. Therefore, the routing metric RM_k^i of node i is defined as follows:

$$RM_k^i = \gamma(SP_k^i \times T_k^i) + (1-\gamma)RE^i, \tag{4}$$

where γ $(0 < \gamma < 1)$ is the parameter to balance the energy, trust and positive progress to the sink.

Based on the routing metric, candidates in Q_k are sorted in the descending order. The first N candidates could be selected in candidate forwarder set, which is denoted as C_k ($C_k \subseteq Q_k$). We further optimize C_k with the scheme in [16] so that all the candidates in C_k are neighbors. We validate the effectiveness of the new routing metric based on our SSI-based trust model in Section VI-B.

3) OPPORTUNISTIC ROUTING

After candidate selection, the source/intermediate node k is ready to send a data packet to the sink. It first performs the selective authentication algorithm (See Section IV-C) to decide to check the data packet or not. When it skips the verification process or the verification result is true, it broadcasts the data packet, which includes the list of candidates and their priorities according to C_k. In the opportunistic routing, each candidate forwarder follows the assigned priority to forward the data packet, as shown in Algorithm 1.

Algorithm 1 Procedure of Opportunistic Routing Run by Candidate Nodes.

```
Input: a data packet broadcast to $N$ candidate nodes with
    their priorities defined by the sender $k$
Output: successful and coordinated data delivery
if Node $i \in C_k$ then
    Receive the data packet;
    Start a timer and $time(i) = \tau * Order(i)$, where $\tau$ is a
    constant and $Order(i)$ is the priority of node $i$ defined
    in the data packet; // $Order(i) = 0, 1, \cdots, N-1$
end if
// Node $i$ is selected as the first candidate node;
if $time(i) == 0$ then
    Node $i$ becomes the next-hop sender, which is ready
    for data transmission;
    return
end if
// Node $i$ is not selected as the first candidate node;
while $time(i)! = 0$ do
    if Node $i$ overhears that the data packet is being trans-
    mitted by another candidate node; then
        Cancel the timer $time(i)$ and drop the data packet;
        return
    end if
end while
// The timer of node $i$ expires
Node $i$ becomes the next-hop sender, which is ready for
data transmission;
return
```

After receiving the data packet correctly, a candidate node i starts a timer $time(i) = \tau * Order(i)$, where τ is a constant and $Order(i)$ is its priority defined in the data packet. Therefore, the higher-priority node has a shorter timer. As a result, the first candidate node instantly turns into the next-hop sender. It would establish its own forwarder set, and prepare for the data transmission.

According to the timers, other low-priority candidate node caches the received data packet and waits for transmission. If it hears that the data packet is being transmitted by another high-priority node, it would cancel the timer and drop the data packet. Once the timer expires, the candidate node becomes the next-hop sender, and prepares for the data transmission. Subsequent sensor nodes carry out the same process until the data packet reaches the sink.

C. SELECTIVE AUTHENTICATION ALGORITHM

Before sending a data packet, each sender node signs the data packet with its ECDSA private key in order to provide the security properties of data integrity and non-repudiation in WSNs. To preserve the computational and energy resources, relay nodes often forward data packets without verification until the sink node checks the signatures of data packets. However, such a forwarding scheme is vulnerable to DoS attacks, where attackers send a large number of bogus data packets with illegal signatures to waste the network resources and disrupt the normal operations of WSNs. Especially, opportunistic routing makes DoS attacks more serious that invalid data packets are reliably delivered with multiple candidate forwarders. The scheme of checking signatures on every node can block the invalid data packets, but it immensely extends the delivery delay and is computationally expensive.

To response the challenge of designing a lightweight authentication scheme for opportunistic routing, we leverage a selective authentication algorithm that can fast block bogus signatures without checking all the signatures at every sensor node. We observe that a received signature can be verified with a lower probability when the sensor node knows more information about the forwarder. Hence, forwarder or neighbor identification should be supported in our algorithm. There are many efficient schemes for neighbor identification (e.g., TESLA [35]), our algorithm works with all of them. As the measurement of uncertainty, node verification probability is exploited to achieve isolation of attackers, which could be adjusted dynamically according to received invalid signatures.

We denote v_y^x as the probability that node y verifies a data packet forwarded by a neighbor node x. Our goal is to update v_y^x, leading to $v_y^x \to 0$ for benign x, and $v_y^x \to 1$ for malicious x. After a period of time, we want to make neighbor nodes of a DoS attacker verify every data packet and neighbor nodes of a benign node verify nothing.

In the neighbor list of a sensor node, each neighbor node is assigned a node verification probability. For example, if node y receives the packet M_x sent by node x and the packet M_z sent by node z, y would check M_x with the probability v_y^x, and M_z with the probability v_y^z. These node verification probabilities should be updated over time.

To initialize the node verification probability, the sensor node could set an initial value for every newly neighbor node. After the initial allocation, the value of node verification probability is able to be adjusted in many ways, such as a linear function and a step function. As suggested in [37], we employ the step function, which maintains v_0 and jumps to one when receiving the threshold number of invalid signatures, to achieve the isolation of DoS attackers. The node verification probability is also affected by receiving warning push, which will be discussed later.

In our implementation, our selective authentication algorithm verifies the first data packet from a new neighbor, and then sets the initial node verification probability to v_0 for later data packets. The links associated with attackers have a high probability of verification over time, and attackers that have sent numerous invalid signatures are blocked from communication. We evaluate the performance of our selective authentication algorithm in Section VI-C and VI-D.

D. COOPERATIVE VERIFICATION SCHEME

Our cooperative verification scheme is proposed to optimally integrate the selective authentication algorithm into trust-based geographic opportunistic routing. When a sensor node decides to verify a data packet, it breaks down the priorities of candidate forwarders defined by the opportunistic routing. This is because the verification time of a signature is much greater than the transmission time [18]. Therefore, we design the mechanism of verification notice to restore the priorities of candidate forwarders in opportunistic routing. After verification, we use the mechanism of warning push to share the verification information of invalid signatures between candidates for efficiency. This enables SelGOR to accelerate the isolation of attackers, and avoid duplicate invalid data transmission or redundant signature verification. Algorithm 2 describes our cooperative verification scheme, which mainly consists of the mechanism of verification notice and the mechanism of warning push.

1) VERIFICATION NOTICE

Based on node verification probability, if a sender or a relay node decides to verify a data packet before transmission, it will broadcast a packet of verification notice, which includes its identity, the data packet's identifier (i.e., the identity of source node and the sequence number), the identities of candidate nodes with low priorities and the estimation of the verification time.

After receiving the verification notice, a candidate node specified in the packet will increase its timer by the verification time. Therefore, candidate nodes with low priorities need to wait for transmission until the signature is verified by the high-priority sensor node. With the reset timers, candidate nodes are reordered according to the priorities assigned in opportunistic routing.

2) WARNING PUSH

If a data packet's signature agrees with the public key of the source node, it would be considered to be a valid data packet, and then forwarded by the relay node with opportunistic routing. Otherwise, it fails the verification and is dropped by the relay node. If an invalid signature is detected, the relay node adjusts the node verification probability of its preceding forwarder. As illustrated in Figure 2, the relay node R_1 increases the node verification probability of node A if M is invalid. Besides, a packet of warning push which contains the relay node's identity, the data packet's identifier, the identity of the preceding forwarder node and the identities of candidate nodes with low priorities, is broadcast by the relay node.

Algorithm 2 Procedure of Cooperative Verification Run by Candidate Nodes

```
if Node $i \in C_k$ becomes the next-hop sender then
    Perform selective authentication algorithm with the output of a flag;
    if The flag indicates verification then
        Broadcast a packet of Verification Notice;
        Verify the data packet;
        if The data packet is invalid then
            Increase node verification probability;
            Broadcast a packet of Warning Push;
            Drop the data packet;
        else
            Send the data packet with opportunistic routing;
        end if
    else
        Send the data packet with opportunistic routing;
    end if
else
    if Node $i$ receives Verification Notice then
        Increase its timer;
    end if
    if Node $i$ receives Warning Push then
        Increase node verification probability;
        Stop its timer and drop the data packet;
    end if
end if
```

Upon receiving the warning push, a candidates node specified in the packet performs two operations. On the one hand, it increases the node verification probability of the preceding forwarder as well. In our example, node R_2 and R_3 increase the node verification probability of A if they receive the warning push from node R_1. On the other hand, the candidate node stops its timer and then drops the data packet.

In contrast to most of the authentication schemes which make each node to verify the data packet independently, SelGOR exploits the shared verification information between neighbors to assist the adjustment of node verification probability for fast isolation. For receiving the shared verification information, other candidate nodes are aware of the invalid data packet. Ultimately, they directly stop the opportunistic transmission and drop the data packet without extra verification, which significantly reduces the cost of bandwidth resources.

V. PRELIMINARY ANALYSIS OF AUTHENTICATION

Since each sender signs every data packet with its private key, the signature of the data packet ensures the properties of data integrity and non-repudiation. Instead of checking every signature on the sensor node, we exploit the selective authentication algorithm to reduce the computational cost in SelGOR. Here, we study the effect of selective authentication algorithm, and consider a simple line model for ease of modeling.

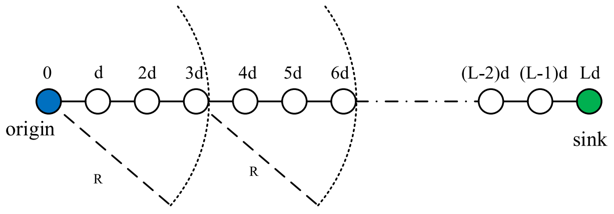


FIGURE 3. A line model of relay nodes with the transmission range R.

As shown in Figure 3, we assume sensor nodes are placed at location $0, d, 2d, \cdots, Ld$. The transmission range R is set to Nd. Therefore, each node has N candidate nodes for data forwarding. The DoS attacker is located at the origin location, and sends an invalid signature at intervals. We consider the attacker sends a valid signature to avoid being detected at the beginning (i.e., $g = 0$), and then sends invalid signatures after the first time interval (i.e., $g = 1$).

When a candidate node $i \in C_s$ receives a data packet from the sender s, it verifies the signature with the verification probability of v_i^s. We denote $F(g, h)$ as the expected number of invalid signatures forwarded h hops from the attacker at time g, where $0 \leq h \leq g$.

First, we analyze the impact of selective authentication algorithm on the primary opportunistic routing. To isolate the DoS attacker, each sensor node independently verifies the signature based on the node verification probability. However, according to the rule of opportunistic routing, the data packet can be successfully forwarded to the next hop node as long as one of candidates skips the process of verification. Hence, $F(g, h)$ of the primary opportunistic routing is calculated as:

$$F_{OR}(g, h) = g * \prod_{s=0}^{h-1}(1 - \prod_{i=0}^{N-1} v_i^s), \tag{5}$$

where $1 - \prod_{i=0}^{N-1} v_i^s$ indicates that the probability of verification skipped by at lease one candidate.

Our protocol exploits cooperative verification scheme to share the verification information between candidates. Therefore, if the first candidate finds an invalid signature, it instantly sends warning push to notice other candidates. Therefore, $F(g, h)$ of our SelGOR is expressed as:

$$F_{SelGOR}(g, h) = g * \prod_{s=0}^{h-1}(1 - v_0^s), \tag{6}$$

where v_0^s indicates the node verification probability of the first candidate node.

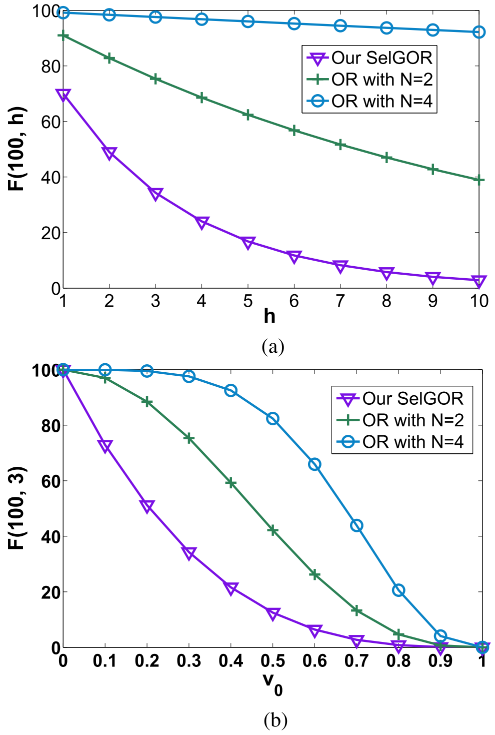


FIGURE 4. The effect of authentication with $g = 100$. (a) F varies with h, when v_0 is set to 0.3. (b) F varies with v_0, when h is set to 3.

Considering that the initial node verification probability is set to v_0 for all nodes, we compare the impact of authentication on our SelGOR with that on primary opportunistic routing in Figure 4. The analysis result shows that SelGOR can converge more rapidly than the primary opportunistic routing with the selective authentication algorithm. As h increases, the number of invalid signatures in Equation (6) decreases much faster than that in Equation (5), since the mechanism of warning push accelerates the isolation process. When v_0 increases, more invalid signatures are dropped at one hop as expected. It is also observed that sinks receive more invalid signatures in primary opportunistic routing with a higher N, which theoretically confirms that DoS attacks pose serious threats to the primary opportunistic routing.

VI. PERFORMANCE EVALUATION

In this section, we perform simulation experiments to evaluate the performance of SelGOR under the DoS attacks in OPNET network simulator. We first describe the simulation setup. Second, we show the reliability of SelGOR, and compare it with other three routing protocols under different link qualities. Third, we study the performance of SelGOR with different parameters. Finally, we provide the simulation results to demonstrate the effectiveness of authentication achieved by SelGOR.

A. SIMULATION SETUP

In our implementation, sensor nodes are placed randomly in the network of 300m×300m. The quality of the wireless link is varied from 0.5 to 1 for our test. Sensor nodes use ECDSA key pairs for signing and verification operations. To avoid being detected, the DoS attacker would sometimes send valid data with legitimate signatures. Hence, we consider the probability of attack rate is varied from 0.1 to 1 in different scenarios.

We use the Nakagami model in the physical layer and the modified version of IEEE 802.11b in the MAC layer to support opportunistic routing. In our test, we only consider the energy cost of signature verification, since it consumes orders of magnitude more energy than transmitting or receiving data packets [18]. Each simulation result is based on 20 iterations. Table 1 lists the default simulation parameters and the sample values commonly used by wireless sensor networks [11], [15], [16], [18].

TABLE 1. Default parameters for simulation.

Parameter	Value
Network size	300m × 300m
Number of nodes	60, 120 or 180
MAC protocol	IEEE 802.11b with 1 Mbps
Transmission range	80m
Link quality	0.8
Probability of attack rate	0.5
Number of flows	10 CBR
Packet size	512 Bytes
Initial power of sensor node	36 mW
Power for signature verification	24 mW
ECDSA verification time	1.62s
Initial node verification probability	$v_0 = 0.1$ or 0.3
Number of candidate nodes	$N = 3$
Time slot	$\tau = 0.01$s
Weight values	$\alpha = 0.9, \omega = 0.7, \gamma = 0.7$

We exploit the following metric to evaluate SelGOR's performance in WSNs:

1) Packet Delivery Ratio (PDR): defined as the ratio of the number of packets received at the sinks to the number of packets sent by the source nodes.
2) Number of Verification: the total number of verification performed by the sensor nodes in the network during the simulation time, which is the indicator of computational cost as well as energy consumption.
3) Hop Count of Invalid Packets: measured as the average hop count of invalid data packets transmitted in the network.
4) Transmission Overhead of Invalid Packets: defined as the total number of invalid packets transmitted in the network (bits).
5) End-to-End Delay: the average time for the data packets delivered from source nodes to sinks, including both the valid and invalid data packets (seconds).
6) Proportion of Invalid Packets: the ratio of the number of invalid data packets received at the sinks to the total number of data packets received at the sinks.
7) Control Packet Overhead: the number of extra packets for data delivery in unit time (bits/s), including the beacon messages, the packet of verification notice and the packet of warning push.

B. THE IMPACT OF LINK QUALITY

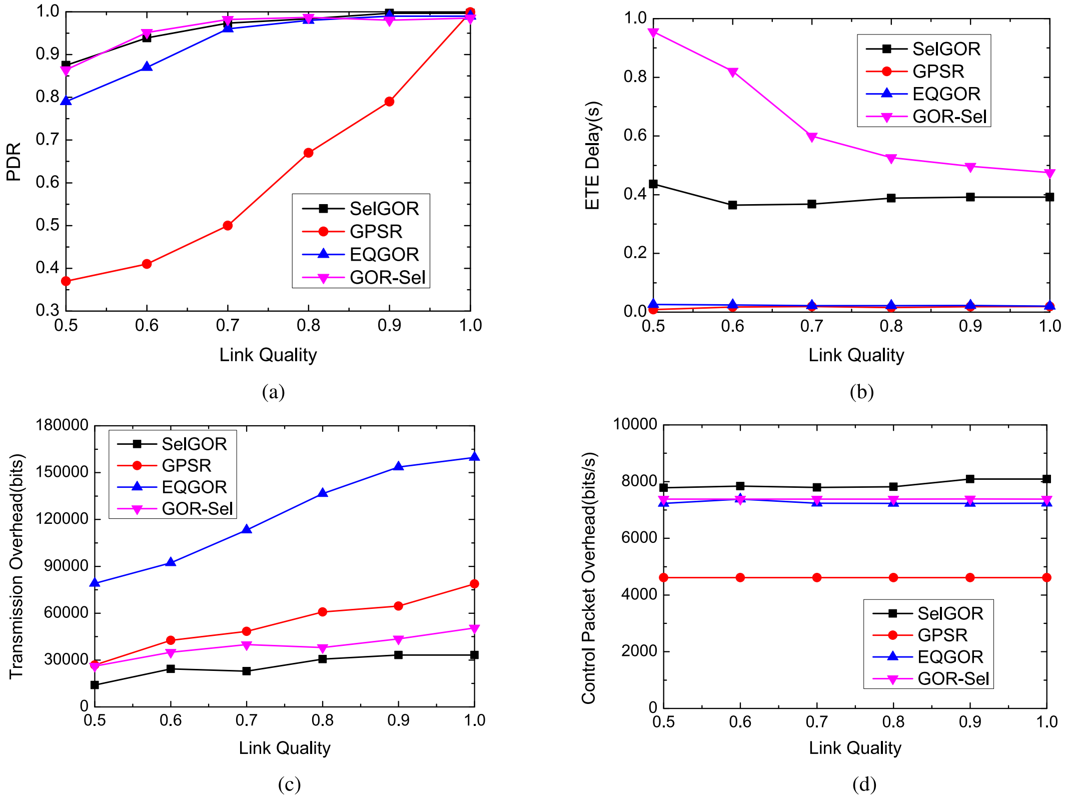
We first evaluate the performance of SelGOR with different link qualities in the 60-node network, and compare it with three other schemes: the single-path routing (i.e., GPSR [13]), the opportunistic routing (i.e., EQGOR [16]) and the opportunistic routing with authentication (i.e., GOR-Sel). For comparison, We introduce GOR-Sel which is constructed by the trust-based geographic opportunistic routing and selective authentication algorithm, but lacks cooperative verification scheme. The node verification probability is set to 0.1. The link quality which indicates the packet reception ratio of the wireless link ranges from 0.5 to 1.

Figure 5(a) shows the packet delivery ratio under different link qualities. As the link quality decreases, many data packets are dropped in the paths and the PDRs of all the schemes decline. Compared with GPSR, opportunistic routing schemes have much higher PDRs since multiple candidates are deployed at each hop for data delivery instead of one forwarder. It is also shown that SelGOR and GOR-Sel perform better than EQGOR, which indicates that integrating our SSI-based trust model into the routing metric could effectively improve the reliability of data delivery.

Figure 5(b) indicates the performance of end-to-end delay under different link qualities. We could see that using authentication in WSNs inevitably increases the delay of data delivery. When there are more packets lost due to poor link quality, it is shown that the delay of GOR-Sel sharply increases. This is because redundant verification has been incurred by opportunistic routing. In this case, GOR-Sel cannot certain the data packet is dropped for being invalid or link failure. With the scheme of warning push, SelGOR could reduce the number of verification and the delay performance is not affected much by the link quality.

Figure 5(c) reports the transmission overhead of invalid packets under different link qualities. It is shown that our SelGOR has the lowest transmission overhead, and significantly preserves the computational resources. With multiple candidate forwarders, EQGOR introduces more than twice of the transmission overhead of GPSR, which experimentally confirms that the DoS attacks are more serious for opportunistic routing.

Figure 5(d) plots the control packet overhead under different link qualities. It is seen that all the opportunistic routing schemes have higher control overhead than GPSR. Since we use the packets of verification notice and warning push to achieve the cooperative verification scheme, the overhead of SelGOR is slightly higher than the other two opportunistic routing schemes. To examine the scalability of SelGOR, we also evaluate the control packet overhead under different number of sensor nodes, as shown in Figure 6. We find that the overhead of the cooperative verification scheme only occupies a tiny proportion of overall control overhead. It means that our SelGOR scheme is scalable with a few communication overhead.



(a)

(b)

(c)

(d)

FIGURE 5. The impact of link quality. (a) Packet Delivery Ratio. (b) End-to-End Delay. (c) Transmission Overhead of Invalid Packets. (d) Control Packet Overhead.

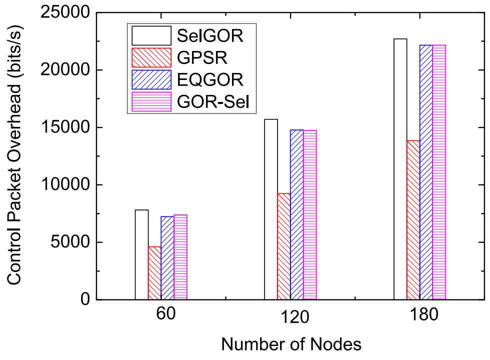


FIGURE 6. Control packet overhead with different number of nodes.

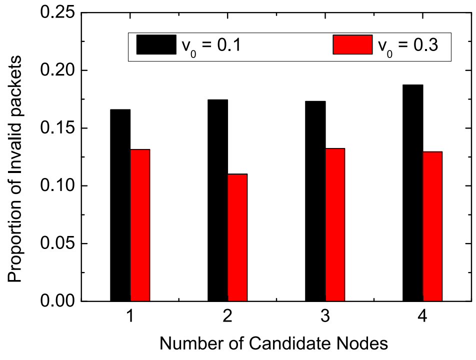


FIGURE 7. The proportion of invalid packets under different number of candidate nodes.

Based on these results, SelGOR performs best, which has the highest packet delivery rate with an acceptable delay even over the poor wireless links. When there are DoS attackers in the network, it could effectively stop at least 70% invalid data packets spreading with a relatively low communication overhead compared to the EQGOR scheme.

C. THE IMPACT OF PARAMETER

We examine how the number of candidate nodes N and the initial node verification probability v_0 affect our scheme in the 120-node network. As a significant parameter in the opportunistic routing, the number of candidate nodes ranges from 1 to 4 for the evaluation of SelGOR.

The proportion of invalid packets is shown in Figure 7. With a higher v_0, the relay nodes increase the number of verification and then filter more invalid data packets. Hence, less invalid packets arrive at the sinks leading to the decrease of the ratio of the number of invalid packets to all the received packets. Therefore, the initial node verification probability plays an important role on the proportion of invalid packets. We also find that the proportion of invalid packets does not change much with the number of candidate nodes. These simulation results correspond to our analysis of Equation (6) in Section V.

TABLE 2. Comparison of five schemes.

Scheme	Geographic Routing	Opportunistic Routing	No Authentication	All Authentication	Selective Authentication	Cooperative Verification
SelGOR	✓	✓			✓	✓
No-Verify	✓	✓	✓			
Verify-All	✓	✓		✓		
GPSR-Sel	✓				✓	
GOR-Sel	✓	✓			✓	

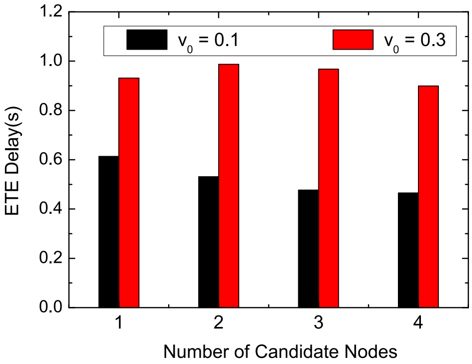


FIGURE 8. The end-to-end delay under different number of candidate nodes.

Figure 8 illustrates the end-to-end delay under different number of candidate nodes. As the initial node verification probability increases, the delay of data packets apparently increases from 0.6 to 1. Although prior work has shown that the increase of the number of candidate nodes could extend the end-to-end delay of data packets in the opportunistic routing [15], the end-to-end delay of our SelGOR does not raise as N increases in our simulation. The reason is mainly that the verification delay of the data packet dominates the end-to-end delay so that such an increase becomes negligible for data delivery. It is observed that the end-to-end delay is significantly influenced by the initial node verification probability.

From the above results, the proportion of invalid packets would decrease with a high v_0. However, such a setting could critically increase the end-to-end delay. Hence, the choice of the initial node verification probability should be determined by the specific requirement of IoT-based applications.

D. THE PERFORMANCE OF AUTHENTICATION

We analyze the performance of authentication under the scenarios of lossless wireless links. In the scenarios, we compare SelGOR with the other four solutions under the topologies with different attack rates of the DoS attackers. These five solutions are now summarized in Table 2: 1) No-Verify is the primary geographic opportunistic routing without authentication scheme. 2) Verify-ALL is the approach where every sensor node verifies each incoming data packet. 3) GPSR-Sel is the common unicast routing GPSR where every sensor node selectively verifies data packets. 4) GOR-Sel makes uses of the selective authentication algorithm without cooperative verification scheme.

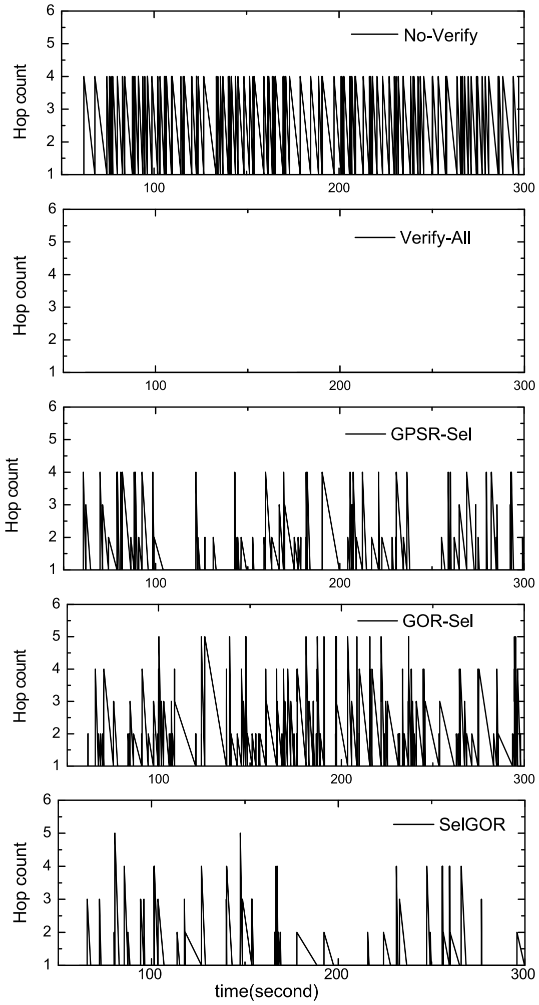


FIGURE 9. Hop count of invalid packets.

Figure 9 shows the effectiveness of authentication in each of the schemes by examining how far the invalid data packets can transfer. In this test, the attacker sends invalid packets with the data rate of 1Hz, and the attack rate is 0.5. The node verification probability for selective authentication algorithm is set to 0.3. It can be observed that Verify-ALL> Our SelGOR > GPSR-Sel > GOR-Sel > No-Verify in terms of the ability to prevent invalid data packets. We also find that GOR-Sel which only uses the selective authentication algorithm does not perform well. With the cooperative verification scheme, SelGOR stops more invalid packets in the network and accelerates the isolation of attackers as we expected. Verify-ALL perfectly blocks all invalid data packets, but it has the very high computational overhead that we will show shortly.

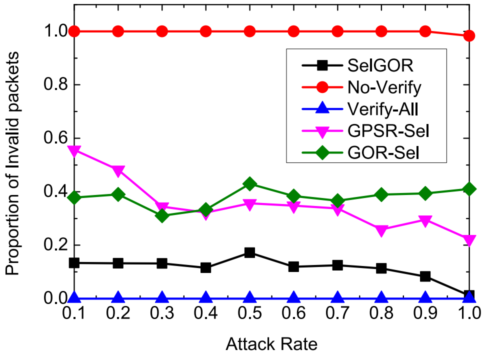


FIGURE 10. **Authentication: the proportion of invalid packets under different attack rates.**

We study the effectiveness of authentication under different scenarios by changing the attack rate from 0.1 to 1. The performance of the proportion of invalid data packets is indicated in Figure 10. Our SelGOR could block more than 80% of invalid data packets, which is better than both GPSR-Sel and GOR-Sel. It is observed that GPSR-Sel which uses one path for data delivery is sensitive to the attack rate. In terms of the proportion of invalid data packets, both our SelGOR and GOR-Sel do not vary much as the attack rate increases, since opportunistic routing exploits multiple candidate forwarders leading to more stable data delivery.

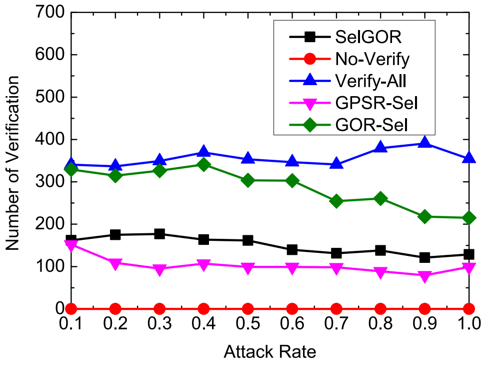


FIGURE 11. **Authentication: the number of verifications under different attack rates.**

Figure 11 shows the number of verification during the simulation time. Since every node verifies the incoming data packet, the computational cost of Verify-All is the highest among the five schemes. By using selective authentication algorithm, GPSR-Sel has a low number of verification. However, for the rule of opportunistic routing, GOR-Sel introduces more than twice the number of verification of GPSR-Sel. Compared with GOR-Sel, our SelGOR apparently reduces the number of verification by 50%, which validates that the cooperative verification scheme could effectively decrease the number of verification caused by opportunistic routing. It is obviously seen that SelGOR reaches the close performance to GOR-Sel, which indicates the high efficiency of our SelGOR.

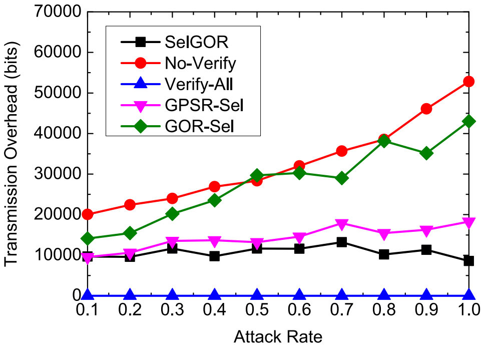


FIGURE 12. **Authentication: the transmission overhead of invalid data packets under different attack rates.**

Figure 12 plots the transmission overhead of invalid packets. We find that GOR-Sel has more transmission overhead of invalid packets than GPSR-Sel. The reason is that the transmission of the invalid data packets is continued although these packets are dropped by some high-priority candidate after verification. Since our SelGOR employs the mechanism of warning push to share the verification result between candidates, it is able to maintain a low transmission overhead of invalid data packets.

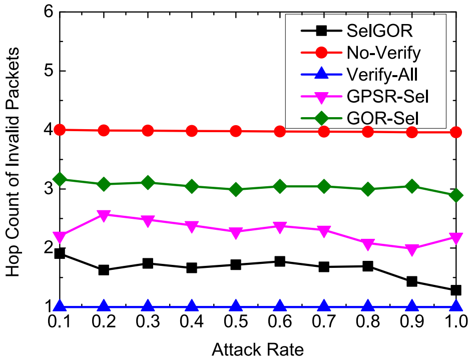


FIGURE 13. **Authentication: the hop count of invalid data packets under different attack rates.**

Figure 13 depicts the hop count of invalid packets among five schemes. The hop count of invalid packets of GOR-Sel is much high and does not vary with the attacker rate. This is because there are duplicate transmissions of invalid data as illustrated in Figure 12. From the simulation result, the hop count of invalid data of SelGOR is much lower than GOR-Sel and GPSR-Sel. It is worth noting that SelGOR efficiently blocks invalid data packets at the first two hops.

As a summary, SelGOR prevents more than 80% of invalid data packets, while it consumes less than 50% of the number of verification compared to the solution of Verify-ALL, and 50% of transmission overhead compared to the solution of No-Verify. The simulation results also highlight that our cooperative verification scheme could significantly decrease the number of verification and transmission overhead raised by the opportunistic routing.

VII. CONCLUSION

In this paper, we designed an efficient scheme SelGOR aiming to provide the properties of authenticity and reliability of data delivery for IoT-based applications. As a trust-based geographic opportunistic routing, SelGOR exploits the SSI-based trust model to improve the reliability of data delivery in WSNs. To defend against DoS attacks, we studied the existing authentication schemes and found that they failed to operate for opportunistic routing due to either being unserviceable or high computational cost in WSNs. Hence, we developed a lightweight selective authentication algorithm to isolate DoS attackers with low computational cost. To cooperate the selective authentication algorithm with the opportunistic routing, we designed a distributed cooperative verification scheme, which could block the spread of invalid data packets and reduce the number of signature verification raised by the opportunistic routing. Extensive evaluations indicate that our SelGOR holds a high packet delivery rate even over poor wireless links. With low communication cost, our SelGOR effectively blocks the DoS attackers while significantly reducing the computational cost compared to other schemes.

From our evaluation results, our protocol runs efficiently with respect to the computational and communication resources. However, the end-to-end delay could become quite long when a high node verification probability is decided. In future work, we will formulate the problem, and study how to adjust the node verification probability to achieve the optimal performance of delay. Another extension of our work is to establish the behavior model of DoS attackers and investigate the improvement of the selective authentication algorithm.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[4] R. H. Weber, "Internet of Things—New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010.

[5] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 6–28, Dec. 2004.

[6] E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: Multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 5, no. 6, pp. 738–754, Jun. 2006.

[7] S. Li, R. K. Neelisetti, C. Liu, and A. Lim, "Efficient multi-path protocol for wireless sensor networks," *Int. J. Wireless Mobile Netw.*, vol. 2, no. 1, pp. 110–130, 2010.

[8] X. Huang and Y. Fang, "Multiconstrained QoS multipath routing in wireless sensor networks," *Wireless Netw.*, vol. 14, no. 4, pp. 465–478, 2008.

[9] G. Schaefer, F. Ingelrest, and M. Vetterli, "Potentials of opportunistic routing in energy-constrained wireless sensor networks," in *Proc. 6th Eur. Conf. Wireless Sensor Netw.*, Cork, Ireland, Feb. 2009, pp. 118–133.

[10] R. Sanchez-Iborra and M. Cano, "JOKER: A novel opportunistic routing protocol," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1690–1703, May 2016.

[11] J. Luo, J. Hu, D. Wu, and R. Li, "Opportunistic routing algorithm for relay node selection in wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 11, no. 1, pp. 112–121, Feb. 2015.

[12] J. So and H. Byun, "Load-balanced opportunistic routing for duty-cycled wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 7, pp. 1940–1955, Jul. 2017.

[13] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Boston, MA, USA, Aug. 2000, pp. 243–254.

[14] K. Zeng, Z. Yang, and W. Lou, "Location-aided opportunistic forwarding in multirate and multihop wireless networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 6, pp. 3032–3040, Jul. 2009.

[15] S. Yang, C. K. Yeo, and B. S. Lee, "Towards reliable data delivery for highly dynamic mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 1, pp. 111–124, Jan. 2012.

[16] L. Cheng, J. Niu, J. Cao, S. K. Das, and Y. Gu, "QoS aware geographic opportunistic routing in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1864–1875, Jul. 2014.

[17] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 74–81, Jan./Mar. 2008.

[18] P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 1, pp. 1–35, 2008.

[19] M. Naghshvar and T. Javidi, "Opportunistic routing with congestion diversity in wireless multi-hop networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–5.

[20] S. Biswas and R. Morris, "ExOR: Opportunistic multi-hop routing for wireless networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 4, pp. 133–144, 2005.

[21] L. Cheng, J. Niu, Y. Gu, T. He, and Q. Zhang, "Energy-efficient statistical delay guarantee for duty-cycled wireless sensor networks," in *Proc. 12th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, 2015, pp. 46–54.

[22] X. Tang, J. Zhou, S. Xiong, J. Wang, and K. Zhou, "Geographic segmented opportunistic routing in cognitive radio ad hoc networks using network coding," *IEEE Access*, vol. 6, pp. 62766–62783, 2018.

[23] M. Salehi and A. Boukerche, "A novel packet salvaging model to improve the security of opportunistic routing protocols," *Comput. Netw.*, vol. 122, pp. 163–178, Jul. 2017.

[24] L. Zhang, J. Song, and J. Pan, "A privacy-preserving and secure framework for opportunistic routing in DTNs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7684–7697, Sep. 2016.

[25] C. Lyu, D. Gu, X. Zhang, S. Sun, Y. Zhang, and A. Pande, "SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs," *Comput. Commun.*, vol. 59, pp. 37–51, Mar. 2015.

[26] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1768–1776.

[27] S. Khanna, S. S. Venkatesh, O. Fatemieh, F. Khan, and C. A. Gunter, "Adaptive selective verification," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Phoenix, AZ, USA, Apr. 2008, pp. 529–537.

[28] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access*, vol. 5, pp. 24012–24022, 2017.

[29] M. Krotofil, A. A. Cardenas, B. Manning, and J. N. Larsen, "CPS: Driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals," in *Proc. 30th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, 2014, pp. 146–155.

[30] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1097–1107, 2011.

[31] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach," *Int. J. Netw. Secur.*, vol. 5, no. 2, pp. 145–153, Sep. 2007.

[32] J. Deng, R. Han, and S. Mishra, "Defending against path-based DoS attacks in wireless sensor networks," in *Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw.*, 2005, pp. 89–96.

[33] S. Hyun, P. Ning, A. Liu, and W. Du, "Seluge: Secure and DoS-resistant code dissemination in wireless sensor networks," in *Proc. IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2008, pp. 445–456.

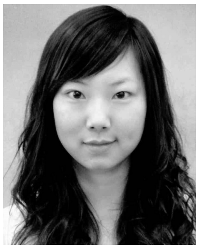
[34] D. He, C. Chen, S. Chan, and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1946–1956, May 2012.

[35] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," in *Proc. NDSS*, 2001, pp. 35–46.

[36] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004.

[37] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J. Hubaux, and J. Le Boudec, "Adaptive message authentication for multi-hop networks," in *Proc. 8th Int. Conf. Wireless Demand Netw. Syst. Services*, Bardonecchia, Italy, 2011, pp. 96–103.

CHEN LYU received the B.S. and M.S. degrees in telecommunications engineering from Xidian University, Xi'an, China, in 2007 and 2010, respectively, and the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2016. She is currently a Lecturer with the Department of Computer Science and Technology, Shanghai University of Finance and Economics, Shanghai, China. Her research interests include wireless security, applied cryptography, and security and privacy in online social networks.



XIAOMEI ZHANG received the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2018. She is currently a Lecturer with the School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai, China. Her publications include more than 30 papers in scholarly journals and conference proceedings. Her current research interests include wireless network security and distributed system security. She is a member of the Shanghai Computer Security.

ZHIQIANG LIU received the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University. He is currently an Associate Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China. His research interests include cryptocurrency and blockchain technology, privacy preserving, design and analysis of symmetric-key cryptography, side-channel attacks, and white-box cryptography.

CHI-HUNG CHI received the Ph.D. degree from Purdue University, West Lafayette. He has worked in industry (Philips Research Laboratory, USA and IBM, Poughkeepsie) and universities (The Chinese University of Hong Kong, the National University of Singapore, and Tsinghua University) for more than 20 years. He is currently a Senior Principal Research Scientist of Data61, Commonwealth Scientific and Industrial Research Organization, Australia. He has published more than 260 international journal and conference papers and edited ten books; he also holds six USA patents. His research interests include cybersecurity, behavior modeling, knowledge graph, data engineering and analytics, cloud and service computing, social computing, the Internet-of-Things, and distributed computing.