



# AHV-RPL: Jamming-Resilient Backup Nodes Selection for RPL-Based Routing in Smart Grid AMI Networks

Taimin Zhang, Xiaoyu Ji, and Wenyan Xu<sup>(✉)</sup>

Zhejiang University, Hangzhou, China  
{zhangtaimin,xji,wyxu}@zju.edu.cn

**Abstract.** Advanced metering infrastructure (AMI) is the core component of the smart grid. As the wireless connection between smart meters in AMI is featured with high packet loss and low transmission rate, AMI is considered as a representative of the low power and lossy networks (LLNs). In such communication environment, the routing protocol in AMI network is essential to ensure the reliability and real-time of data transmission. The IPv6 routing protocol for low-power and lossy networks (RPL), proposed by IETF ROLL working group, is considered to be the best routing solution for the AMI communication environment. However, the performance of RPL can be seriously degraded due to jamming attack. In this paper, we analyze the performance degradation problem of RPL protocol under jamming attack. We propose a backup node selection mechanism based on the standard RPL protocol. The proposed mechanism chooses a predefined number of backup nodes that maximize the probability of successful transmission. We evaluation the proposed mechanism through MATLAB simulations, results show the proposed mechanism improves the performance of RPL under jamming attack prominently.

**Keywords:** Smart grid · Advanced metering infrastructure (AMI) · Jamming · RPL

## 1 Introduction

Advanced metering infrastructure uses tremendous smart meters as sensing devices to collect user's power usage information, and also as auxiliary devices for power grid monitoring. Smart meters usually adopt wireless technologies for data transmission. Due to the complex and varying electromagnetic environment of the smart meters' installation location, the wireless connection between smart meters are featured with of high packet loss and low transmission rate. Therefore, AMI is considered as a representative of the low power and lossy networks

---

Supported by National Key R&D Program of China (2018YFB0904900, 2018YFB0904904).

(LLNs) [1]. In the AMI network communication environment, ensuring reliable and real-time transmission of data is a challenging task, and the key factor to achieve this goal is efficient and robust routing algorithms.

A large amount of research on routing protocols in AMI networks have been conducted, among which IPv6 routing protocol for low-power and lossy networks (RPL) [2] proposed by the IETF ROLL working group is considered to be the best candidate. The aim of the RPL protocol was to overcome routing problems in resource-constrained devices, and security has not been paid enough attention to. Jamming attack is a common attack in wireless networks, it is easy to conduct while can degrade the network's transmission performance severely. In RPL networks, the network topology update frequency is low, and each node transmits data to the data center using a single default node (named preferred parent) as the next hop. When jamming attack causes the preferred parent node's failure, the packet loss rate will increase rapidly. On the other hand, the transmission frequency of RPL networks' control packets is low, so the network topology repair process after the jamming attack is slow. Renofio et al. [3] simulated the performance of an 80-node AMI network implementing RPL protocol under jamming attack. The results show that the repair time of the network topology significantly exceeds the duration of the jamming attack. Considering the low cost and easy-to-implement features of jamming attacks, it poses a significant security threat to RPL networks.

For the above-mentioned jamming attacks, the most easy while efficient defense method is to select backup nodes for each node in the RPL network. When the preferred parent node is no longer available, the RPL node can continue the data transmission by switching to the backup nodes when jamming attack happens, thereby improving the overall transmission performance of the network. Backup nodes selection mechanisms have been studied in existing work to improve RPL networks' transmission performance in congestion scenarios [4–6]. However, backup nodes selection in jamming attack scenarios is essentially different to that in congestion scenarios. The congestion problem is caused by the excessive communication load. The probability of being congested is independent on different nodes. Therefore, increasing backup nodes can increase the probability of successful transmission. In jamming attack scenarios, the probability of transmission failure on different nodes is not independent. If both the preferred parent node and the backup node are within the jamming range, it is very likely that transmission failure will occur on the two nodes at the same time when jamming attack happens. In the rest of this paper, we refer to this phenomenon as the fault correlation between different RPL nodes. Therefore, simply increasing number of backup nodes does not necessarily increase the probability of successful transmission under jamming attack. It is necessary to consider the fault correlation while selecting backup nodes in order to maximize the possibility of successful transmission.

In this paper, we propose AHV-RPL, a backup nodes selection mechanism that can improve the performance of standard RPL protocol under jamming attack. To solve the above-mentioned fault correlation problem, we propose a

fault correlation calculation method based on the availability history vector (AHV) metric proposed by Mustafa et al. [7]. The proposed mechanism constructs a backup nodes set with the least fault correlation, thus the routing performance of the RPL network under jamming attack can be improved. The main contributions of this paper are as follows:

- We propose a novel backup nodes selection mechanism based on the standard RPL protocol. Compared to other backup nodes selection methods, the proposed mechanism can choose backup nodes that have minimum fault correlation to the preferred parent node, thus increases the probability of successful transmission under jamming attack.
- We propose an efficient AHV delivery mechanism for the RPL’s DODAG (Destination Oriented Direct-ed Acyclic Graph) construction process. In this mechanism, each node can calculate its own AHV based on the AHV information it received from the parent nodes.
- The proposed mechanism is evaluated through MATLAB simulations. Results show that our backup nodes selection mechanism can improve the RPL’s transmission performance under jamming attack evidently.

We organize the remainder of the paper as follows. In Sect. 2, we discuss the related work. We introduce jamming attack models and formulate the problem in Sect. 3. In Sect. 4, we present our framework for backup nodes selection and give implementation of our algorithms. In Sect. 5, we validate the proposed mechanism through MATLAB simulations. Finally, we conclude in Sect. 6.

## 2 Related Work

### 2.1 RPL Background

The RPL protocol is a distance vector routing protocol for low-power lossy networks. Its design follows the topology concept of directed acyclic graphs. Objective function (OF) is used to map the network into multiple non-coincident destination oriented directed acyclic graphs (DODAGs). DODAG has a tree topology and each DODAG corresponds to one root node (DODAG root). All paths point to the root node, which is generally used as a data aggregation node or as a gateway node to connect to an external network (such as Internet).

In order to form a DODAG, each node that has joined the RPL network (referred to as RPL node in the rest of the paper) is assigned with a rank value. Nodes with high rank values select nodes with lower rank values as their parent node, and the root node has the lowest rank value in the DODAG. The rank value of the node is calculated according to the Objective Function (OF). The commonly used objective function is MRFOF developed by the IETF ROLL Working Group [8]. Assume that the node  $N_j$  is the parent node of node  $N_i$ , then the rank value of node  $N_i$  can be calculated according to MRFOF function:

$$R(N_i) = R(N_j) + ETX(N_i, N_j) \quad (1)$$

where  $R(x)$  represents the rank value of node  $x$  in DODAG, and  $ETX$  (Expected Transmission Count) is a route metric defined as:

$$ETX = \frac{1}{D_f \times D_r} \quad (2)$$

where  $D_f$  refers to the probability that node  $N_i$  successfully transmits a packet to node  $N_j$ , and  $D_r$  refers to the probability that node  $N_i$  successfully receives the packet from node  $N_j$ . The smaller the  $ETX$ , the better the link quality between the node  $N_i$  and node  $N_j$ , and the higher the packet transmission rate. Conversely, the larger the  $ETX$ , the more unstable the link.

A node that has not joined the RPL network needs to select one of the neighboring RPL nodes as the preferred parent node. Then the node can join the network through the preferred parent node. In order to select a preferred parent node, the node first needs to receive the DODAG Information Object (DIO) messages broadcasted by other RPL nodes. Then it extracts the rank value of the source node and the objective function (OF) from the DIO message. The node can calculate its own rank value based on the source node's rank and the OF. Assume that node  $N_i$  receives multiple DIO messages from  $m$  RPL nodes, and let  $\mathcal{N}_r = \{N_{r_1}, N_{r_2}, \dots, N_{r_m}\}$  represents the set of  $m$  RPL nodes. For  $N_{r_m} \in \mathcal{N}_r$ , the node  $N_i$  calculates its own rank value according to Eq. 1, and obtains a set  $\mathcal{R} = \{R_1, R_2, \dots, R_m\}$ . In this set, node  $N_i$  selects the minimum value as its own rank value and selects the corresponding node as the preferred parent node.

After all nodes have selected the preferred parent node, the construction of the RPL network topology is completed. And all RPL nodes transmit data to the root node through their preferred parent nodes, this process is called uplink data transmission. When the preferred parent node is unavailable, each RPL node needs to reselect the preferred parent node through the repair mechanism.

## 2.2 RPL Security

The RPL protocol is considered to be the most suitable routing protocol for smart grid communication scenarios. At present, there are a lot of work to study the application of RPL protocol in smart grid environment [9–13]. Although the RPL protocol has broad application prospects in the smart grid, some research also pointed out the security problems of the RPL protocol. Zaidi et al. [14] studied the RPL black hole attack. The attacker uses malicious nodes to attract normal traffic in the network and discard all received packets, which has a great impact on network transmission performance. Mayzaud et al. [15] studied the version number attack against RPL. By using malicious nodes to broadcast malicious messages with manipulated version numbers to the RPL network, the network topology is reorganized and formed. This attack can cause a large number of routing loops, which can reduce the network's life. Wallgren et al. [16] pointed out the harm of identity theft attacks against RPL. The attacker uses malicious nodes to simultaneously clone the identity information of multiple legitimate nodes in the network, thereby achieving the purpose of controlling a large number of nodes on the network. To defend this attack, the RPL nodes needs to

be authenticated in combination with the identity information of the node and the registered location information. In addition, wormhole attacks, sybil attacks, and sinkhole attacks in normal wireless sensor networks are also applicable to networks based on RPL routing protocols [17].

### 2.3 Availability History Vector (AHV)

Mustafa et al. proposed the available history vector (AHV) metric to evaluate the network performance under jamming attack [7]. AHV uses a sequence of bit 0 and bit 1 to represent the availability of a link (or a path) in a past period of time. Specifically, bit 0 means the link (or path) is jammed and can not be used for data transmission, and bit 1 means the link (or path) is available for data transmission.

An efficient way to obtain the AHV of a link is to map the packet delivery rate (PDR) into bit 0 and bit 1 by comparing the PDR with a predefined threshold. Packet delivery rate (PDR) refers to the ratio of successfully transmitted data packets to the total number of transmitted data packets. If node  $N_i$  transmits data packets to node  $N_j$ , the link PDR between node  $N_i$  and node  $N_j$  can be defined as:

$$PDR = \frac{C_r}{C_s} \quad (3)$$

where  $C_s$  is the total number of packets sent by the  $N_i$  node, and  $C_r$  is the total number of packets received by the  $N_j$  node.

The path AHV can be calculated based on the link AHV. The details of calculating AHVs are given as follows.

- **Link AHV calculation.** As mentioned above, link AHV can be obtained by mapping the link PDR into bit 1s and bit 0s. Specifically, let  $A_{i,j}$  be the link between node  $N_i$  and node  $N_j$ . The AHV of link  $A_{i,j}$  can be denoted as  $\mathbf{a}_{i,j} = [a_{i,j}^1, a_{i,j}^2, \dots, a_{i,j}^t]$ .  $a_{i,j}^t$  represents the availability of link  $A_{i,j}$  at time  $t$  and it can be calculated by comparing it to a threshold  $\theta$ :

$$a_{i,j}^t = \begin{cases} 1, & PDR_i \geq \theta \\ 0, & PDR_i < \theta \end{cases} \quad (4)$$

- **Path AHV calculation.** The path AHV is derived from the link AHVs. Assume path  $H_j$  is composed of  $i$  links denoted as  $A_1, A_2, \dots, A_i$ . Let  $\mathbf{a}_i = [a_{i,j}^1, a_{i,j}^2, \dots, a_{i,j}^t]$  be the AHV of link  $A_i$ , and  $\mathbf{h}_j = [h_j^1, h_j^2, \dots, h_j^t]$  be the AHV of path  $H_j$ . Let  $\wedge$  be the bit “and” operation, then the path AHV can be derived from the link AHV:

$$\begin{aligned} \mathbf{h}_j &= [h_j^1, h_j^2, \dots, h_j^t] = \mathbf{a}_1 \wedge \mathbf{a}_2 \wedge \dots \wedge \mathbf{a}_i \\ h_j^t &= a_1^t \wedge a_2^t \wedge \dots \wedge a_i^t \end{aligned} \quad (5)$$

- **Combination AHV calculation.** In practice, there are usually more than one path between the source node and the destination node. Let  $V$  be

the combination of several path between the source node and the destination node, AHV is also capable of representing the availability history of the path combination  $V$ . Assume the path combination  $V$  is composed of path  $H_1, H_2, \dots, H_j$ . Let  $\mathbf{h}_j = [h_j^1, h_j^2, \dots, h_j^t]$  be the AHV of path  $H_j$ , and  $\mathbf{v} = [v^1, v^2, \dots, v^t]$  be the AHV of combination  $V$ . Let  $\vee$  be the bit “or” operation, then the combination AHV can be derived from the path AHV:

$$\begin{aligned}\mathbf{v} &= [v^1, v^2, \dots, v^t] = \mathbf{h}_1 \vee \mathbf{h}_2 \vee \dots \vee \mathbf{h}_j \\ v^t &= h_1^t \vee h_2^t \vee \dots \vee h_j^t\end{aligned}\quad (6)$$

### 3 Problem Formulation

#### 3.1 Jamming Attack

The jamming attack utilizes the open nature of the wireless channel and transmit jamming signal at the same frequency as the RPL nodes. This will lead to error bits in the transmitted packets. Thus the data packets cannot pass the verification on the receiver side and will be discarded.

According to the jamming behavior, jammer can be classified into active jammer and reactive jammer [18]. Active jammers do not consider network channel conditions, and use persistent jamming signals to block communication between network nodes. Such attacks can be easily detected. Reactive jammers keep silent when the channel is idle, and transmit jamming signals when there is data transmission on the channel. Due to the stealthy characteristic of reactive jammers, they are more difficult to be detected. The mechanisms designed in this paper are primarily designed to defend RPL networks from reactive jammers.

The signal noise ratio (SNR) indicator is generally used to measure the intensity of the jamming attack. SNR refers to the ratio of the normal signal strength to the jamming signal strength, which is defined as:

$$SNR = \frac{P_S}{P_N} \quad (7)$$

where  $P_S$  is the strength of the normal signal and  $P_N$  is the strength of the jamming signal.

If presented in decibels (dB), Eq. 7 is converted to:

$$SNR(dB) = 10 \log_{10} \frac{P_S}{P_N} = P_{d_S} - P_{d_N} \quad (8)$$

where  $P_{d_S} = 10 \log_{10} P_S$  and  $P_{d_N} = 10 \log_{10} P_N$ .

In general, there is a positive correlation between  $PDR$  and  $SNR$ . That is, as  $SNR$  increases, the value of  $PDR$  rises. The mapping between  $SNR$  and  $PDR$  can be obtained by mathematical derivation. At a given  $SNR$ , the probability of a transmission error for each bit of the transmitted data is  $Q\sqrt{2kE_b/N_0}$  [19], where  $k \approx 0.85$ .  $E_b/N_0$  is the ratio of the average signal strength to the noise signal strength when transmitting each bit of data, and its value is the same as

the signal to noise ratio  $SNR$ . The function  $Q(\cdot)$  represents the probability that the random variable  $X$  in the Gaussian distribution  $X \sim N(0, 1)$  is greater than the threshold  $z$ , namely:

$$Q(z) \triangleq p(X > z) = \int_z^\infty \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy \tag{9}$$

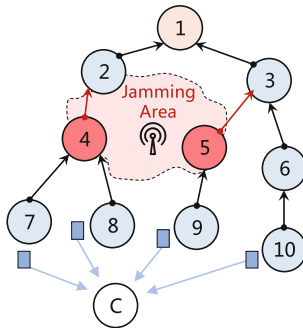
Since the process of erroneous transmission of each bit is independent of each other, assuming that the data packet transmitted between node  $N_i$  and node  $N_j$  is  $M$  bits, the above mapping relationship can be used to derive the link  $PDR$  between the node  $N_i$  and the node  $N_j$  as:

$$PDR = \prod_{i=1}^M (1 - Q(\sqrt{2kSNR^i})) \tag{10}$$

where  $SNR^i$  corresponds to the signal-to-noise ratio when transmitting the  $i$ th bit.

### 3.2 Failure Correlation

Since the jammer has a certain transmission range, the communication of all nodes located within the jamming range will be affected when jamming attack occurs. Not only the nodes located in the jamming range are affected, nodes that transmit data through the affected nodes will not be able to transmit data. We name this phenomena as fault correlation. As shown in Fig. 1, nodes 4 and 5 lose communication with their preferred parents when jamming attack occurs, so nodes 4 and 5 are fault correlated.



**Fig. 1.** An example of the fault correlation between node 4 and node 5.

As each node in RPL network selects only a single preferred parent node to transmit data to the root node, if two RPL nodes are fault correlated, their child nodes also have the same fault correlation characteristics. As shown in Fig. 1, node 4 and node 5 are subject to reactive jamming attacks. When the jammer is

not active, assume that node C selects node 8 as its preferred parent node, and it selects a backup node from node 7, 9 and 10. If node C selects node 7 or node 9 as the backup node, it will not be able to send data to the root node when jamming attack happens. That is because node 7, node 8 and node 9 are fault correlated since their parent nodes (node 4 and node 5) are fault correlated. If node C selects node 10 as the backup node, it can quickly switch to node 10 and maintain communication with the root node when jamming occurs.

In order to facilitate the quantitative analysis of fault correlation, we adopted the availability history vector (AHV) metric proposed by Mustafa et al. [7]. By continuously recording the link availability according to Eq. 4, a time-varying sequence  $\mathbf{a} = [a^1, a^2, \dots, a^t]$  can be obtained, which is the AHV. More generally, assuming that there is a communication path  $H$  between node  $N_i$  and node  $N_j$ , the path can be either a single-hop link or a path composed of multiple links. Then the AHV of the path  $H$  can be defined as  $\mathbf{h} = [h^1, h^2, \dots, h^t]$ , where  $h^t \in 0, 1$  represents the availability of path  $H$  at time  $t$ .

Based on the AHVs defined above, fault correlation can be calculated quantitatively. Notice that there are multiple different paths between node  $N_i$  and node  $N_j$ . For example, in Fig. 1 there are different paths between node C and node 1, such as C-7-4-2-1, C-8-4-2-1 and C-9-5-3-1 etc. Assume that the AHVs of two paths  $H_k$  and  $H_n$  are  $\mathbf{h}_k = [h_k^1, h_k^2, \dots, h_k^t]$ , and  $\mathbf{h}_n = [h_n^1, h_n^2, \dots, h_n^t]$ . Let  $\wedge$  denote the bitwise *and* operator, and  $\neg$  denote the bitwise *not* operator. Then the fault correlation between paths  $H_k$  and  $H_n$  can be defined  $\phi(H_k, H_n)$ :

$$\phi(H_k, H_n) = \sum_{i=1}^t \neg h_k^i \wedge \neg h_n^i \quad (11)$$

As the fault correlation between paths  $H_k$  and  $H_n$  become higher, more bit 0 will occur on the same positions in  $\mathbf{h}_k$  and  $\mathbf{h}_n$ , thus the value of the metric  $\phi(H_k, H_n)$  becomes larger. And the lower the fault correlation, the lower the value of the metric  $\phi(H_k, H_n)$ . Further, the metric can be extended to calculate the fault correlation of a set of paths  $\mathcal{H} = \{H_1, H_2, \dots, H_k\}$ . Let  $\phi(\mathcal{H})$  denote the fault correlation of the path set  $\mathcal{H}$ , then:

$$\phi(\mathcal{H}) = \sum_{i=1}^t \left( \bigwedge_{j=1}^k \neg h_j^i \right) \quad (12)$$

## 4 Design

The existing backup node selection mechanisms for the RPL protocol are not applicable to the jamming attack situation. The main reason is that the fault correlation between the RPL nodes is not considered in these mechanisms. Based on the AHV definitions and fault correlation metric, we propose AHV-RPL, a backup nodes selection mechanism for the RPL protocol's resistance against jamming attacks.



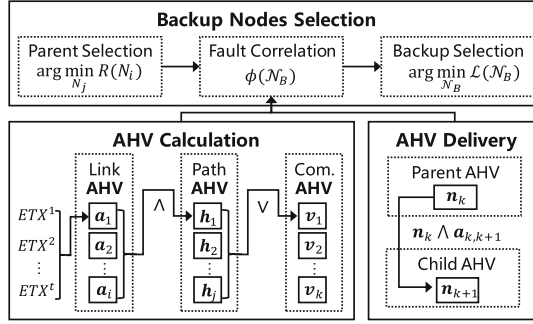


Fig. 2. The framework of AHV-RPL.

#### 4.1 Overview of AHV-RPL

The framework of AHV-RPL is shown in Fig. 2. The proposed AHV-RPL mainly contains three process, i.e. the AHV calculation process, the AHV delivery process, and the backup nodes selection process.

In the AHV calculation process, each node calculate link AHV, path AHV and combination AHV according to Eqs. 4 to 6. The standard RPL protocol uses the metric  $EXT$  instead of  $PDR$  to indicate the link quality. However, we can map the metric  $EXT$  in to link AHV in a similar way to Eq. 4. Let  $\mathbf{a} = [a^1, a^2, \dots, a^t]$  denote the AHV of a link, then it can be calculated based on the link's  $EXT$  at different times:

$$a^t = \begin{cases} 1, & EXT \leq \theta \\ 0, & EXT > \theta \end{cases} \quad (13)$$

where  $EXT$  is defined in Eq. 2 and  $\theta$  is a predefined threshold. Based on the link AHV, path AHV and combination combination AHV can be efficiently calculated.

Each RPL node can easily calculate the link AHV based on the metric  $EXT$ . To calculate path AHV and combination AHV, each node have to obtain path AHV from its parent nodes and deliver the path AHV to its children node. During the DODAG construction process, each RPL node obtains a path AHV from its preferred parent, and calculates the AHV of the link between itself and the parent node. Then it updates the path AHV and deliver it to its children node. By doing so, each RPL node in the network can maintain a link AHV and a path AHV.

The backup nodes selection process is used in the DODAG construction process of the standard RPL protocol. After selecting the preferred parent node, the fault correlation calculation is performed on each RPL node to select a set of backup nodes that has the least fault correlation with the preferred parent.

The improved AHV-RPL protocol enables the RPL node to quickly switch to the backup nodes for uplink data transmission when the RPL network is subjected to jamming attack, thereby improving the overall anti-jamming ability of the network.

**Algorithm 1.** Node AHV Delivery

---

```

1: Input : Node AHV  $\mathbf{n}_{i-1}$  of the preferred parent  $N_{i-1}$ ,
2: Output : Node AHV  $\mathbf{n}_i$  of the preferred parent  $N_i$ ,
3: Procedures :
4: if Node  $N_i$  is the root node then
5:   Initializing  $\mathbf{n}_0 = [n_0^1, n_0^2, \dots, n_0^t]$ .
6:   For  $n_0^i \in \mathbf{n}_0$ , set  $n_0^i \leftarrow 1$ .
7:   Broadcasts DIO message that contains  $\mathbf{n}_0$ .
8: else
9:   Receive DIO message from node  $N_{i-1}$ .
10:  Extract  $\mathbf{n}_i$  from DIO message.
11:  Calculate link AHV  $\mathbf{a}_i$ .
12:  Update node AHV  $\mathbf{n}_i = \mathbf{n}_{i-1} \wedge \mathbf{a}_i$ .
13:  Broadcasts DIO message that contains  $\mathbf{n}_i$ .
14: end if

```

---

**4.2 AHV Delivery**

The proposed backup nodes selection mechanism requires RPL nodes to obtain calculate the AHV of its default path to the root node. However, each RPL node can only obtain the link AHV information from the surrounding nodes within its receiving range. Therefore, in the process of constructing DODAG, a delivery mechanism of the path AHV is needed. So that each RPL node can calculate the AHV of its own default path to the root node from its parent node's DIO message.

For each RPL node, its default path to the root node is composed of a sequence of preferred parent nodes and is settled once the DODAG is constructed. Thus, we can define node AHV as the AHV of a node's default path to the root node. For node  $N_i$ , assume its default path to the root node is composed of the node set  $\mathcal{N} = \{N_1, N_2, \dots, N_i\}$ , where  $N_{i-1}$  is the preferred parent of  $N_i$ . Let  $\mathbf{a}_{i-1,i}$  denote the AHV of link  $A_{i-1,i}$ , and  $\mathbf{a} = [a_{i-1,i}^1, a_{i-1,i}^2, \dots, a_{i-1,i}^t]$ . Then the node AHV of node  $N_i$  is defined as:

$$\begin{aligned} \mathbf{n}_i &= [n_i^1, n_i^2, \dots, n_i^t] = \mathbf{a}_{0,1} \wedge \mathbf{a}_{1,2} \wedge \dots \wedge \mathbf{a}_{i-1,i} \\ n_i^t &= a_{0,1}^t \wedge a_{1,2}^t \wedge \dots \wedge a_{i-1,i}^t \end{aligned} \quad (14)$$

where  $a_{0,1}$  represents the link AHV between the root node (denoted as  $N_0$ ) and node  $N_1$ .

For a concise representation, we represent  $\mathbf{a}_{i-1,i}$  as  $\mathbf{a}_i = [a_i^1, a_i^2, \dots, a_i^t]$ . From the definition of node AHV, we can see that the AHV of each RPL node can be recursively derived from the node AHV of its preferred parent:

$$\begin{aligned} \mathbf{n}_i &= [n_i^1, n_i^2, \dots, n_i^t] = \mathbf{n}_{i-1} \wedge \mathbf{a}_i \\ n_i^t &= n_{i-1}^t \wedge a_i^t \end{aligned} \quad (15)$$

In the above method for calculating the node AHV, RPL nodes receive DIO messages broadcast by their parent node during the DODAG construction process. Each RPL node updates and maintains its own node AHV information

according to their parent nodes' AHV. Then, they transmit their node AHV information downward through DIO messages. The process is shown in Algorithm 1. First, the root node initializes its own node availability vector  $n_0$ , where  $n_0 = [1^1, 1^2, \dots, 1^t]$ . That is, the availability of the root node at each moment is always of value 1. From Eq. 15, we can see that along the path number of bit 1 in the node AHV of the child node is reduced compared to the parent node's AHV, which means the overall usability is degraded.

### 4.3 Backup Nodes Choosing

To defend against jamming attacks, each RPL node have to select several backup nodes after selecting the preferred parent during the DODAG construction process of the standard RPL protocol. When a RPL node loses communication with its preferred parent due to jamming attack, it can quickly switch to a backup node and maintain data transmission towards the root node. This section presents the details of the proposed backup nodes selection mechanism. When the DODAG construction process is completed, each RPL node will be able to maintain several fault-independent backup nodes along with the preferred parent node.

The backup nodes selection process can be divided into two steps. First, assuming that the node  $N_i$  has selected the preferred parent node  $N_{p_0}$  and calculated its own Rank. Node  $N_i$  can choose nodes with lower rank value among the neighbor nodes as the candidate backup nodes, thereby obtaining a candidate backup node set  $\mathcal{N}_P = \{N_{p_1}, N_{p_2}, \dots, N_{p_k}\}$ . Then node  $N_i$  selects  $q$  nodes from the candidate backup node set  $\mathcal{N}_P$  to form a back node set  $\mathcal{N}_B = \{N_{b_1}, N_{b_2}, \dots, N_{b_q}\}$ ,  $\mathcal{N}_B \subseteq \mathcal{N}_P$ . The AHV of the backup node set is denoted as  $\mathbf{m}_B$ .

The requirement for the backup node set  $\mathcal{N}_B$  is that the fault correlation metric  $\phi(\mathcal{N}_B)$  is as small as possible. In order to calculate the fault correlation metric  $\phi(\mathcal{N}_B)$ , node  $N_i$  is first required to calculate its node AHV  $\mathbf{n}_{b_q+1}$  according to each parent node  $N_{b_q} \in \mathcal{N}_B$ . Then node  $N_i$  calculates the AHV  $\mathbf{m}_B$  of the parent node set  $\mathcal{N}_B$  based on the AHVs  $\{\mathbf{n}_{b_1+1}, \mathbf{n}_{b_2+1}, \dots, \mathbf{n}_{b_q+1}\}$  obtained in the last step. Let  $A_{b+q,i}$  denote the link between node  $N_{b_q}$  and node  $N_i$ , and its link availability is  $\mathbf{a}_{b_j,i}$ . According to Eq. 15, when node  $N_i$  selects node  $N_{b_q}$  as the parent node, its own node AHV is:

$$\begin{aligned} \mathbf{n}_{b_q+1} &= [n_{b_q+1}^1, n_{b_q+1}^2, \dots, n_{b_q+1}^t] = \mathbf{n}_{b_q} \wedge \mathbf{a}_{b_q,i} \\ \mathbf{n}_{b_q+1}^t &= n_{b_q}^t \wedge a_{b_q,i}^t \end{aligned} \quad (16)$$

Referring to the calculation method of the combination AHV, the AHV of the alternate parent node set  $\mathcal{N}_B$  can be derived from Eq. 16.  $\mathbf{m}_B$  can be expressed as:

$$\mathbf{m}_B = [m^1, m^2, \dots, m^t] = \bigvee_{j=1}^q \mathbf{n}_{b_j} \wedge \mathbf{a}_{b_j,i} \quad (17)$$

Based on the AHV of the above-mentioned backup node set, the fault correlation metric  $\phi(\mathcal{N}_B)$  of the backup node set  $\mathcal{N}_B$  can be defined as:

$$\phi(\mathcal{N}_B) = \sum_{i=1}^t \left( \bigwedge_{j=1}^q -n_{b_j+1}^i \right) \quad (18)$$

At the same time, we want the overall availability of the backup node set  $\mathcal{N}_B$  to be as large as possible. Thus, we denote the overall availability metric as  $\psi_{\mathcal{N}_B}(\mathbf{m}_B)$ , which is defined as:

$$\psi_{\mathcal{N}_B}(\mathbf{m}_B) = \sum_{i=1}^t m^i \quad (19)$$

The proposed mechanism for the backup node set  $\mathcal{N}_B$  requires the fault correlation metric  $\phi(\mathcal{N}_B)$  to be as small as possible, the overall availability index  $\psi_{\mathcal{N}_B}(\mathbf{m}_B)$  to be as large as possible. Therefore, we can define an optimization function  $\mathcal{L}(\mathcal{N}_B)$  as:

$$\mathcal{L}(\mathcal{N}_B) = \frac{\phi(\mathcal{N}_B)}{\psi_{\mathcal{N}_B}(\mathbf{m}_B)} \quad (20)$$

The process of forming the above-mentioned back node set  $\mathcal{N}_B$  can be described as an optimization problem that minimizes the optimization function  $\mathcal{L}(\mathcal{N}_B)$ :

$$\begin{aligned} & \arg \min_{\mathcal{N}_B} \mathcal{L}(\mathcal{N}_B) \\ & s.t. \mathcal{N}_B \subseteq \mathcal{N}_P \end{aligned} \quad (21)$$

The mechanism proposed in this section solves the above optimization problem and selects a back parent node set for each node in the DODAG construction process. To solve this optimization problem, a greedy algorithm is used. At each step, the RPL node selects a candidate backup node that minimizes the optimization function  $\mathcal{L}(\mathcal{N}_B)$  and adds it to the backup node set. The details are shown in Algorithm 2.

## 5 Evaluation

The performance of the proposed AHV-RPL protocol is evaluated through MATLAB simulations. In order to demonstrate the effectiveness of the proposed mechanism under jamming attacks, the performance of AHV-RPL is compared with the standard RPL protocol. At the same time, in order to reflect the superiority of the proposed mechanism compared to the existing backup nodes selection mechanism, we set up a greedy backup node selection mechanism as reference. In the greedy backup node selection mechanism, each RPL node selects nodes with highest node availability as the back nodes after choosing the preferred parent node. The simulation results show that the proposed mechanism preforms better than the greedy backup nodes selection mechanism under jamming attack.

---

**Algorithm 2.** Backup Nodes Selection
 

---

- 1: **Input** : Candidate Node Set  $\mathcal{N}_P$ ,
  - 2: **Output** : Backup Node Set  $\mathcal{N}_B$ ,
  - 3: **Procedures** :
  - 4: Initialize  $\mathcal{N}_P = \emptyset, \mathcal{L}(\mathcal{N}_B) = 0, k = 1$ .
  - 5: **while**  $k \leq q$  **do**
  - 6:     Choose node  $N_{p_k} \in \mathcal{N}_P$  that minimize  $\mathcal{L}(\mathcal{N}_B \cup N_{p_k})$ .
  - 7:     Add node  $N_{p_k}$  to  $\mathcal{N}_B$ .
  - 8:     Update  $\mathcal{L}(\mathcal{N}_B) = \mathcal{L}(\mathcal{N}_B \cup N_{p_k})$ .
  - 9:     Delete node  $N_{p_k}$  from  $\mathcal{N}_P$ .
  - 10:     $k \leftarrow k + 1$
  - 11: **end while**
- 

**Table 1.** Definition of the parameters in simulation

Parameter	Meaning	Value
$L$	Size of AMI network	500 m
$P_J$	Transmit power of jammer	25 mW
$P_T$	Transmit power of smart meter	10 mW
$G$	Gain of the antenna	1
$P_N$	Power of ambient noise	-80 dBm
$f_T$	Signal frequency	2.4 GHz
$\eta$	Path loss exponent	2.40

### 5.1 Simulation Setup

The simulation simulates a 60-node RPL network with node locations randomly distributed in the range  $[0, 500] \times [0, 500]$ , as is shown in Fig. 3. The entire network constitutes a directed acyclic graph where node 1 is the root node. The arrows between the nodes represent the communication links. Table 1 shows the parameter values set during the simulation.

In order to evaluate the performance of the proposed mechanism, we define the end-to-end *PDR* of RPL node  $N_i$  as:

$$PDR_i = \frac{C_{r_i}}{C_{s_i}} \quad (22)$$

where  $C_{s_i}$  represents the total number of packets sent by the node  $N_i$  to the root node, and  $C_{r_i}$  represents the total amount of packets received by the root node from the node  $N_i$ . Based on Eq. 22, assume that there are  $n$  RPL nodes in the network, then the average end-to-end *PDR* of the RPL network can be defined as:

$$PDR_A = \frac{1}{n} \sum_{i=1}^n PDR_i \quad (23)$$

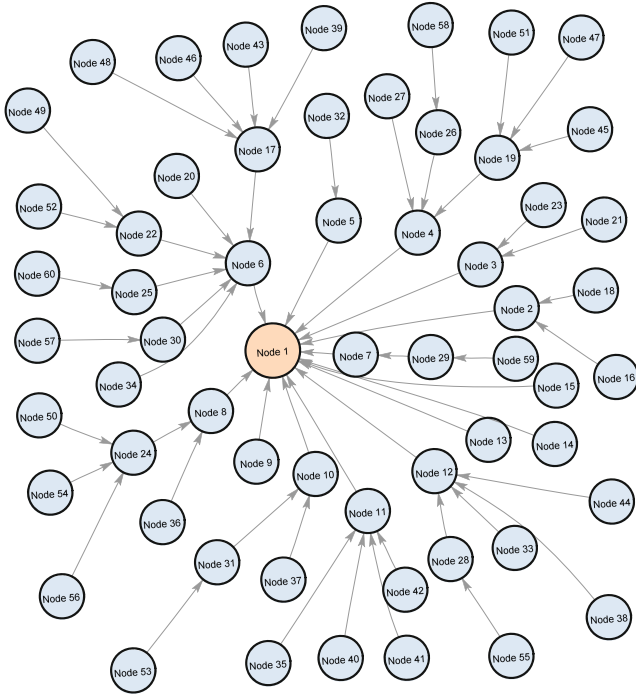


Fig. 3. Topology of the simulated RPL network.

### 5.2 Results

Using the defined average end-to-end packet delivery rate evaluation metrics, we compares the improved AHV-RPL protocol with the standard RPL protocol under jamming attacks. In order to reflect the superiority of the proposed mechanism over existing backup nodes selection mechanism, we setup a greedy backup node selection mechanism. In the greedy backup node selection mechanism, each node selects nodes with the lowest ETX value as the backup nodes.

Figure 4 shows the average end-to-end packet delivery rate of the network when the number of candidate nodes  $N$  is different under the jamming attack. The standard RPL (named ‘Original’ in the figure) is used as a reference. As the number of candidate nodes  $N$  increases, the performance of the greedy backup node selection (named ‘Greedy’ in the figure) and the proposed AHV-RPL (named ‘AHV’ in the figure) are improved. The performance of the proposed AHV-RPL is better than that of the greedy backup node selection. When the number of backup nodes reaches three, the performance of the proposed AHV-RPL is 39.7% higher than that of the greedy backup node selection algorithm, and the average packet delivery rate is 14.6 times that of the standard RPL algorithm.

Figure 5 shows the effect of the jammer’s transmit power on the performance of the proposed algorithm. Assuming that the number of backup parent nodes for each node is 3, the jammer’s transmit power is set to a different value between

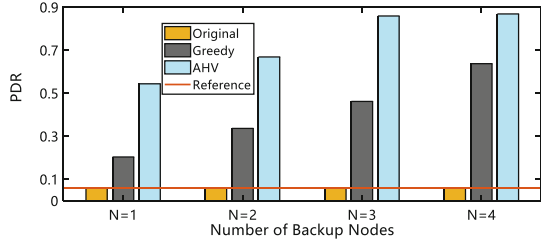


Fig. 4. Impact of number of backup nodes.

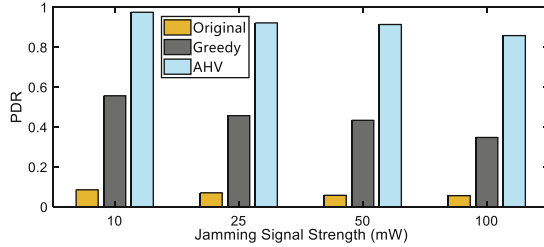
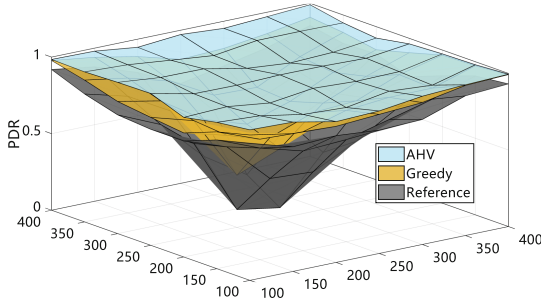


Fig. 5. Impact of jamming signal strength.

10 mW and 100 mW, and the power of the normal node is 10 mW. It can be found that the performance of the greedy backup node selection algorithm and the proposed AHV-RPL algorithm are attenuated as the signal strength of the jammer increases. When the interference source transmission power is 100mW, the average end-to-end packet delivery rate of the proposed AHV-RPL algorithm is still above 85%, and the greedy alternate node selection algorithm is reduced to less than 35%. When the jammer’s transmit power is increased from 10mW to 100mW, the packet delivery rate of the greedy backup node selection algorithm is reduced by 21%, and the AHV-RPL algorithm is reduced by 11%. It can be seen that the robustness of the AHV-RPL algorithm is better than that of the greedy backup node selection algorithm.

Figure 6 shows the impact of jammer’s location on the average end-to-end packet delivery rate of the whole network. Assume that the number of whole parent nodes of each node is 3, the jammer’s transmit power is 10mW, and the normal node power is 10mW. The root node of the network is at (235, 254), and the  $x$  and  $y$  coordinates of the interferer are set to different values between 100 and 400, respectively. It can be found that the closer the location of the jammer is to the root node, the lower the average end-to-end packet delivery rate of the standard RPL and the greedy backup node selection algorithm. This is because RPL nodes close to the root node have a large number of child nodes. When these RPL nodes are interfered, the sub-nodes have strong fault correlation, so the performance of standard RPL and the greedy backup is degraded. The proposed AHV-RPL mechanism takes into account the characteristics of fault correlation, so its performance is less affected by the location of the jammer.

The experimental results show that the average end-to-end packet delivery rate of the AHV-RPL algorithm is higher than 85% no matter where the jammer is, and its performance is better than the standard RPL and greedy backup node selection algorithm.



**Fig. 6.** Impact of jammer's position.

## 6 Conclusion

The RPL routing protocol in the smart grid is vulnerable to jamming attack, and the data transmission performance of the network will be greatly affected under jamming attack. An easy while efficient defense method to defend RPL network against jamming attacks is to select backup nodes for each node in the RPL network. Existing backup node selection mechanisms for the RPL protocol are mainly to solve the load balancing problem and it not applicable to the jamming attack scenario. In view of the above problems, this paper proposed an improvement mechanism for the RPL protocol. We analyzed and modeled the performance degradation problem of RPL network under jamming attack. Based on the AHV metric, the fault correlation between nodes can be quantitatively analyzed using our the fault correlation metric we developed. Based on this, a backup nodes selection mechanism is proposed to construct a backup node set with the least fault correlation for each RPL node. When the preferred parent node of a RPL node fails due to the jamming attack, it can quickly switch to the backup node and continue data transfer towards the root node. Finally, the performance of the proposed AHV-RPL are evaluated through MATLAB simulations. The results show that the proposed mechanism can greatly improve the performance of the standard RPL protocol under jamming attack.

## References

1. Ancillotti, E., Bruno, R., Conti, M.: RPL routing protocol in advanced metering infrastructures: an analysis of the unreliability problems. In: Proceedings of the Sustainable Internet and ICT for Sustainability, SustainIT, Pisa, Italy, pp. 1–10 (2012)
2. Winter, T., et al.: RPL: IPv6 routing protocol for low-power and lossy networks. IETF RFC 6550 (2012)



3. Renofio, J.R.R., Pellenz, M.E., Jamhour, E., Santin, A.O., Penna, M.C., Souza, R.D.: On the dynamics of the RPL protocol in AMI networks under jamming attacks. In: Proceedings of the IEEE International Conference on Communications, Kuala Lumpur, Malaysia, pp. 1–6. ICC (2016)
4. Pavkovic, B., Theoleyre, F., Duda, A.: Multipath opportunistic RPL routing over IEEE 802.15.4. In: Proceedings of the International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems, MSWiM, Miami, Florida, USA, pp. 179–186 (2011)
5. Duquenooy, S., Landsiedel, O., Voigt, T.: Let the tree bloom: scalable opportunistic routing with ORPL. In: Proceedings of the ACM Conference on Embedded Network Sensor Systems, SenSys, Roma, Italy, pp. 2:1–2:14 (2013)
6. Tahir, Y., Yang, S., McCann, J.A.: BRPL: backpressure RPL for high-throughput and mobile iots. *IEEE Trans. Mob. Comput.* **17**(1), 29–43 (2018)
7. Mustafa, H.A., Zhang, X., Liu, Z., Xu, W., Perrig, A.: Jamming-resilient multipath routing. *IEEE Trans. Depend. Secur. Comput.* **9**(6), 852–864 (2012)
8. Gnawali, O., Levis, P.: The minimum rank with hysteresis objective function. IETF RFC 6719 (2012)
9. Ancillotti, E., Bruno, R., Conti, M.: The role of the RPL routing protocol for smart grid communications. *IEEE Commun. Mag.* **51**(1), 75–83 (2013)
10. Ropitault, T., Lampropulos, A., Pelov, A., Toutain, L., Vedantham, R., Chiumiento, P.: Doing it right - Recommendations for RPL in PLC-based networks for the Smart Grid. In: Proceedings of the IEEE International Conference on Smart Grid Communications, pp. 452–457. SmartGridComm, Venice, Italy (2014)
11. Ho, Q., Gao, Y., Rajalingham, G., Le-Ngoc, T.: Robustness of the routing protocol for low-power and lossy networks (RPL) in smart grid's neighbor-area networks. In: Proceedings of the IEEE International Conference on Communications, pp. 826–831. ICC, London, United Kingdom (2015)
12. Yang, Z., Ping, S., Sun, H., Aghvami, A.: CRB-RPL: A Receiver-Based Routing Protocol for Communications in Cognitive Radio Enabled Smart Grid. *IEEE Trans. Veh. Technol.* **66**(7), 5985–5994 (2017)
13. Lemercier, F., Montavont, N.: Performance Evaluation of a RPL Hybrid Objective Function for the Smart Grid Network. In: Proceedings of the International Conference on Ad Hoc Networks and Wireless, ADHOC-NOW, pp. 27–38. Saint-Malo, France (2018)
14. Zaidi, S.A.R., Ghogho, M.: Stochastic geometric analysis of black hole attack on smart grid communication networks. In: Proceedings of the IEEE International Conference on Smart Grid Communications, SmartGridComm, Tainan, Taiwan, pp. 716–721 (2012)
15. Mayzaud, A., Badonnel, R., Chriment, I.: A distributed monitoring strategy for detecting version number attacks in RPL-based networks. *IEEE Trans. Netw. Serv. Manag.* **14**(2), 472–486 (2017)
16. Wallgren, L., Raza, S., Voigt, T.: Routing attacks and countermeasures in the RPL-based Internet of Things. *IJDSN* **9**(8) (2013)
17. Kamgueu, P.O., Nataf, E., Djotio, T.N.: Survey on RPL enhancements: a focus on topology, security and mobility. *Comput. Commun.* **120**, 10–21 (2018)
18. Wei, X., Wang, Q., Wang, T., Fan, J.: Jammer localization in multi-hop wireless network: a comprehensive survey. *IEEE Commun. Surv. Tutorials* **19**(2), 765–799 (2017)
19. Rappaport, T.S.: *Wireless Communications - Principles and Practice*. Prentice Hall, Upper Saddle River (1996)