Research on Secure Data Transmission Algorithm Based on Confidence of Wireless Opportunistic Networks for Energy Internet

Yaofu Cao¹*, Xiaomeng Li¹, Junwen Liu¹, Chengwei Li¹, Junlu Yan¹, Jingcheng Zhao¹

¹ State Grid Information & Telecommunication Branch., Beijing, China
*Corresponding author’s e-mail: yaofu-cao@sgcc.com.cn

Abstract. The Energy Internet is a leading development direction for the modernized and intelligent transformation of the power grid, and a new type of infrastructure that supports the high-quality development of the economy and society. With the access of a variety of mobile terminals, security is one of the most important challenges faced in the construction of Energy Internet. Research on reliable networking and data forwarding strategies on the edge is of great significance to its development. On the basis of analyzing the requirements of typical application scenarios, we introduce in this paper a secure data transmission algorithm based on confidence of wireless opportunistic networks for Energy Internet to resist the influence of malicious behaviours. The simulations of real scenes confirm the advantages of introducing our algorithm on parameters such as the success rate and the delay of data transmission.

1. Introduction
At the beginning of 2020, State Grid Corporation of China decided to take "A internationally leading Energy Internet enterprise with Chinese characteristics" as the company's strategic goal. Energy Internet is a very inclusive concept that is under development and represents a higher stage of power grid development.

The Energy Internet was proposed by Rifkin j. in the third industrial revolution [1] for the first time, and then its definition, network architecture and system composition were constantly enriched and improved by overseas and domestic scholars. The academic community generally believes that the Energy Internet is a complex network system who based on the smart grid as the core, with new energy technologies and information technology as the basis and deeply integrated with multi-energy networks, transportation networks and information networks.

Regarding the goal of the State Grid, we put more emphasis on supporting the clean and low-carbon transformation of electricity energy and the flexible and convenient access of multiple entities, to create a smart energy system with features such as interconnection, multi-energy complementation, efficient interaction, and smart openness [2]. Among them, energy is the fundamental and subject, internet is the method and means. Technically speaking, it is the extensive and in-depth application of modern information and communication technologies such as the "Big data, Cloud, Internet of Things, Mobile computing and Blockchain" in the power system, and the integration and development of advanced power energy technologies to promote the digital, automated, and intelligent characteristics of system operation and management. Promoted by the development of the Energy Internet, the future development of power business will present the service attribute of the Internet of Things, which has the
characteristics of massive terminal access, high reliability, low latency, and high security protection level. Therefore, this will put forward high-quality wireless access requirements and challenges.

The key to achieving the Energy Internet is to further establish physical interconnection, information interconnection and commercial interconnection on the basis of existing renewable energy power generation and smart grid technologies [3]. The cornerstone of information interconnection is Information Communication Technology (ICT) [4]. Since the 1990s, the development of ICT has shown the characteristics of high performance, wide fields and multiple directions. In the future, it will continue to move towards digitalization, integration, intelligence, and networking. Network technology is accelerating the development of wireless, and intelligence and safety. In the future, information networks will cover all types of terminals at the end of the power grid to enhance the "last mile" perception.

![Energy Internet and network security](image)

Figure 1. Energy Internet and network security

### 2. Wireless communication at the edge of the Energy Internet and information security

The application scenarios of wireless communication at the edge of the Energy Internet can be generally divided into two categories: production and management. For example, emergency communication, Internet of vehicles and new energy terminal access scenarios are selected for production services, and mobile inspection (mobile terminals, inspection robots, UAV) and video surveillance are selected as typical scenarios for management services.

However, while mobile applications based on wireless communication networks have brought many conveniences to Energy Internet, they have also enabled the rapid expansion of the boundaries of power networks and information systems, causing a series of security challenges. Therefore, ensuring the timeliness, effectiveness and reliability of the "last mile" wireless network system is an important technical support for the Energy Internet. In terms of information, we should focus on the prevention methods of malicious behaviour intrusion, the privacy protection of information transmission and storage, and the interference of information transmission is also worthy of attention.

It is necessary to build a "ubiquitous, full coverage" power communication network that is safe and reliable, flexible access, and two-way real-time interaction.

In this paper, we propose a secure data transmission algorithm based on confidence of wireless opportunistic networks for Energy Internet, providing advanced, reliable, efficient and secure emerging wireless networking communication technology and support for the Energy Internet. With gradually transformation from simple passive satisfaction of business needs to active leadership of information security needs, we provide a better end-to-end self-control method for network access, carrying and safeguard of multi-scenario business applications in smart grid.
3. Opportunistic network and application scenarios

The opportunistic network is a particular network capable of choosing the right network algorithms at the right time and which could be seen as a mixture of delay-tolerant networks (DTNs) and mobile ad hoc networks. It is not a question of designing a complete path between the source and destination nodes, but of carrying out the inter-node communication so as to carry out the “store-carry-transfer” sequence according to the nodes encountered depending on the mobility of the nodes [5]. In this chapter, we analyse two typical application scenarios in which the technology of opportunity network can be take advantage of in Energy Internet.

3.1. Emergency communication scenario

In Energy Internet, the rapid development of distributed energy and microgrids not only increases the diversity of energy networks, but also increases the complexity of grid configuration and management, which puts forward new requirements for the safe operation of the grid. In the face of natural disasters or emergency events such as earthquakes, floods, freezing, rain and snow, how to improve the robustness of the smart grid poses a new test for the power emergency communication system. The power grid emergency communication system is to comprehensively utilize various communication resources when the power communication is interrupted due to natural disasters or emergency events during the production process of the power system, and build a temporary and rapid response special communication mechanism in the shortest time. So as to minimize the impact and loss caused by the emergency.

The opportunistic network is composed of multiple mobile nodes, all mobile nodes have equal status, and no need mobile communication system base station or access point in the wireless local area network and other similar infrastructures. The most important feature of the mobile nodes of opportunistic network is the routing function, which allows them to form a wireless communication network covering a larger area through "multi-hop" without infrastructure. It has the characteristics of independent networking, rapid deployment, dynamic topology, strong scalability, support for high-speed movement, and interconnection with heterogeneous networks, which can effectively meet the time urgency, network timeliness, location uncertainty, communication business diversity, high degree of autonomy, and network security requirements of emergency communication system for Energy Internet. Therefore, the opportunistic network is suitable as the end subnet of the smart grid emergency communication system.

3.2. UAV line inspection scenario

Unmanned Aerial Vehicle line inspection scenario is mainly aimed at checking the physical characteristics of the transmission lines between the grids, such as bending deformation, physical damage and other characteristics. This scenario is generally used in the open field scenes of high-voltage power transmission, and the distance is relatively long. Generally, the length of the line between two poles and towers is in the range of 200-500 m, and the inspection range includes several poles and towers, which stretch for several thousand meters. Typical applications include channel forest detection, icing monitoring, wildfire monitoring, early warning detection of external damage, etc. In the traditional way, the 2.4G public frequency band WIFI or the manufacturer’s private protocol communication is mainly used between the console and UAVs, and the effective control radius is generally less than 2 km [6]. By introducing opportunistic network, an UAV can use all available communication terminals in environment or other UAVs to form ad hoc network. This enables UAVs to ensure business continuity in the absence of public base stations, realize remote control, and return high-definition video beyond the line of sight, which greatly expands the line inspection range and improves efficiency. The networked UAV inspection can reduce the cost of manual inspection, greatly increase the inspection range, and greatly improve the safety of the work environment for personnel in remote and high-risk environments.
4. Secure data transmission algorithm based on confidence

Transmission or routing is the key issue of opportunistic network, and it is necessary to ensure the confidentiality, reliability and integrity of the message. In general, in the packet forwarding process, certain authentication mechanisms are used to authenticate the source and integrity of data by intermediate nodes due to the demand for security. But the certificate authentication mechanism is not appropriate in an intermittent situation like the opportunistic network.

Malicious node is an umbrella term for nodes that secretly eavesdrop on, intercept or tamper with messages from other nodes. As an important infrastructure, the electric power system faces a particularly interests by malicious node, and unfortunately, the various applications of Energy Internet would further exacerbate the serious threat in this regard. Therefore, ensuring the security and reliability of the opportunistic network for Energy Internet is a key research issue.

In a real business environment, malicious behaviors from nodes severely affect normal network operation, and traditional authentication and protection mechanisms are not enough to effectively resist such behaviors. However, as part of a basic protection strategy [7], trust, it is possible to predict the following behavior through records of historical node behaviors. In addition, the quantified concrete value that represents reliability between nodes is presented to prevent attack from malicious nodes.

Due to the heavy intermittence of communication, trust assessment and storage will only be done between the nodes themselves without the aid of monitoring third-party. And because opportunistic network nodes are always on the move, the assessment process begins first when nodes meet. The algorithm must therefore be designed in a simple and efficient way to ensure that the process is completed in a very short period of time, on the one hand in order to provide enough time for the data transmission, and on the other hand to save energy consumption. We propose our trust model, which is a more efficient mechanism to provide security in the opportunistic network of Energy Internet.

4.1. Data transmission algorithm based on dynamic community similarity of nodes

In the opportunistic network of Energy Internet, speed, direction and trajectory etc. of the nodes are all controlled by the equipment necessary of the business scenario. At the same time as the equipment, for example new energy vehicles or inspection robots, build the relationship through their activities, the possibility of establishing the relationship tie is also provided. So, we can determine the trust relationship between the nodes by comparing the trajectory similarity.
In order to accurately describe the mobile trajectory of the node, it is necessary to divide the entire network into different zones. We divide the network into square subzones of 200\( m \times 200m \) and assign a mark to all the small square areas. In the memory of each node, a two-dimensional matrix table is configured with the same number of divisions as given above. \( T_{ij} \) is a position table of the node which is used to record the path of node. We assume that initially all the items of \( T_{ij} \) are 0. For the current and transient subzones, we mark them with 1, thus we can obtain the trajectory. After the meeting of the nodes, \( T_{ij} \) will be transformed into a matrix of position \( M_{T_{ij}} \), and the nodes exchange their matrix of position, and then respectively calculate the similarity of trajectory, it is shown by the value of cosine including angle:

\[
TS(T_i, T_j) = \frac{M_{T_i} \cdot M_{T_j}}{\|M_{T_i}\| \cdot \|M_{T_j}\|}
\]  

(1)

With the incessant movement of the nodes, the calculation of the trajectory should be updated to ensure that the current trajectory properly represents recent passage subzones. Each node records the previous entry time \( t_{en} \) of a subzone, the previous exit time \( t_{ex} \), and the current time \( t_{cur} \). Only if the update value \( UV(t_{en}, t_{ex}, t_{cur}) \) is below the threshold \( \varphi \), the label of this subzone in the position table will be reset to 0, otherwise will remain at the original state:

\[
UV(t_{en}, t_{ex}, t_{cur}) = e^{-\left(\text{round}(t_{cur}-(t_{ex}-t_{en}))\right)}
\]  

(2)

### 4.1.1. Similarity of relationship

Under normal circumstances, the number of mutual friends of different members of society may in some sense illustrate the strength of the relationship between them [8], in the same way, the terminals in Energy Internet have the more “friends” in common, the stronger their relationship they own. Thus, we can compare the similarity of relationship between the opportunistic network nodes which reflects the relationship of trust.

We use the adjacency list to record the number of interaction nodes in the subzones, the head node of the adjacency list is made up of the subzone data field and the pointer that points to the first node of the adjacency list. The node in the list is made up of the neighboring nodes field, the data field comprising the name of the interaction nodes and the pointer. If node \( i \) has an interaction with node \( b \) and node \( u \) in zone 1 respectively, nodes \( b \) and \( u \) will be added after zone 1 following the order of meeting, which means that node \( i \) has two notes of interaction in zone 1.

Like the node location list, each item in the relationship list corresponds to the network division area, and the adjacent linked list is placed in each subzone. If node \( i \) and node \( j \) meet, they first exchange their matrix of relationship \( M_{R_{ij}} \), and the relationship similarity of the nodes can then be calculated:

\[
RS(R_i, R_j) = \frac{M_{R_{ij}} \cdot M_{R_{ij}}}{\|M_{R_{ij}}\| \cdot \|M_{R_{ij}}\|} \cdot e^{-\text{round}(t_n-t_i)}
\]  

(3)

We assume that the interaction time since the last interaction between nodes is \( t_i \), \( e^{-\text{round}(t_n-t_i)} \) means the degree of weakening of social relation between nodes \( i \) and \( j \), the longer the time without interaction, the greater the degree of attenuation.

### 4.1.2. Confidence level of nodes

In our secure opportunistic network, we can determine the confidence between the nodes by comparing the similarity of trajectory and relationship. We use a weighted sum to integrate the two, and the confidence level of node \( j \) for node \( i \) is \( C_{i,j} \) :

\[
C_{i,j} = \alpha \cdot TS(T_i, T_j) + \beta \cdot RS(R_i, R_j)
\]  

(4)

The weight control of \( \alpha \) and \( \beta=1-\alpha \) here must take into account the subjectivity and the evolutionary characteristic of the assessment of the confidence, the weight distribution method is calculated:
\[
\alpha = \frac{RS(R_iR_j)}{RS(R_iR_j) + TS(T_iT_j)}
\]  

(5)

4.1.3. Confidence-based transmission process

After completing the node confidence assessment, the trusted node should be selected for the next hop in the data transmission. Our algorithm examines the confidence stability according to the historical trust evaluation value of the nodes to choose the trusted node as the forwarding one.

We assume that the sequence of the historical confidence value from node i to node j is \(C_{i_1,j}, C_{i_2,j}, C_{i_3,j}, C_{i_h,j}\), \(h\) signifying the number of times there was a confidence evaluation of node i over node j, the method of calculating its stability is expressed:

\[
\bar{C}_{i,j} = \frac{1}{p} \sum_{h=1}^{p} C_{i_h,j}
\]  

(6)

\[
S_{i,j} = \frac{1}{p} \sum_{h=1}^{p} (C_{i_h,j} - \bar{C}_{i,j})^2
\]  

(7)

Formula (6)(7) first uses the historical confidence value of node i over node j to calculate the mean confidence assessment value of \(p\) times \(\bar{C}_{i,j}\). The variance \(S_{i,j}\) is hence the confidence stability of the node. Finally, to compare the variance \(S_{i,j}\) between the different nodes, if the variance is smaller, the stability and reliability in the relationship of trust between nodes is better.

The specific process of confidence-based transmission can be divided into several stages:

1. Calculate the confidence value of each node with the other nodes in its communication field \(C_{i,j}\), and then calculate the mean confidence evaluation value \(\bar{C}_{i,j}\) and the variance \(S_{i,j}\) of the other nodes thanks to the historical trust value of this node.
2. According to the mean confidence value \(\bar{C}_{i,j}\), select nodes which have an average confidence value greater than the value of the confidence threshold \(C_\theta\), i.e. \(C_{i,j} \geq C_\theta\), and put them in the set of nodes \(TempN_h = \{N_h\}\).
3. Observe the variance \(S_{i,j}\) of the node in the set of nodes \(TempN_h\), order them from the smallest to the largest, and choose the node of the smallest.

5. Experiment

In order to verify the proposed confidence transmission algorithm, we use the 'Opportunistic Network Environment (ONE)' [9] as simulation software. In order to measure the efficiency of the proposed algorithm, we select the transmission success rate and the average delay time as evaluation parameters.

We take advantage of the parameters similar to the real situation of the scenario of the city of Helsinki and simulate square areas that can be divided into subzones of 200m * 200m. 200 nodes are installed for simulation, using Bluetooth communication between them, communication radius of 10m, node movement speed of [1-3] km / h, data transmission rate of 200Kbps.

Figures 5, 6, and 7 respectively compare in the network coverage of 1000m * 1000m, 2000m * 2000m, 3000m * 3000m and with a different ratio of malicious nodes, the success rate of the three transmission modes of commonly used classical algorithms Epidemic [10], Prophet [11] and Spray-and-Waits [12] in the absence and with our confidence algorithm.
We can see that in the case of the addition of our confidence algorithm, although the trend of the success rate decreases as the ratio of malicious nodes increases, however, thanks to the trust relationship
established by the confidence strategy, the reliability of data transmission is effectively ensured, which reduces the influence of malicious nodes in the process of data transmission.

Representatively, we test the average delay time of the three transmission modes in an area of 3000m * 3000m with and without adding our algorithm. By adding our algorithm, the mean transmission delay time is effectively reduced, that is, the tendency to increase the mean delay time is well attenuated.

Figure 6: The mean delay time in 3000m * 3000m area

The experimental results showed that the proposed secure data transmission algorithm based on confidence can improve the transmission success rate and reduce data delay times. By using the algorithm in the opportunistic network of Energy Internet, the data security of the network is well ensured taking into account the performance of the network at the same time.

6. Conclusion
In this paper, we have presented firstly the background of current Energy Internet. Secondly, we have introduced wireless communication at the edge of the Energy Internet and the importance of information security. Thirdly, opportunistic network and its typical application scenarios in Energy Internet was proposed. And finally, an algorithm using confidence to improve the strategy of data transmission in the opportunistic network of Energy Internet has been detailed, and particularly as a countermeasure to malicious nodes. The simulations of real scenarios confirm the advantages of the introduction of our algorithm on certain parameters such as the success rate and the delay of data transmission.

Our work still has limitation, the total number of intelligent terminals in Energy Internet is actually huge, not to mention the amount of user-generated connections, interactions and content. However, this paper did not take into account the scaling problem and only evaluated our proposed algorithms and approaches on data sets of limited scale. This could lead to many difficult problems to deal with, and will likely require techniques from other areas of research such as distributed systems and parallel computing. Therefore, another direction for our future research is to adapt the algorithm we propose to scalable approaches that can be exploited in more scenarios and platforms made up of a very large number of terminals or nodes in Energy Internet.

Acknowledgments
This work is supported by The Science & Technology Project of State Grid Information & Telecommunication Branch.

References
[1] J. Rifkin. “The third industrial revolution: how lateral power is transforming energy and changing the world,” in the economy and the world, New York, USA, 2011
[2] WU Kehe, WANG Jiye, LI Wei, et al. Research on the operation mode of new generation electric power system for the future energy internet[J]. Proceedings of the CSEE, 2019, 39(4): 966-978(in Chinese).

[3] SHU Yinbiao, XUE Yusheng, CAI Bin, et al. A review of energy transition analysis part two uncertainties and approaches[J]. Automation of Electric Power Systems, 2018, 42(10): 1-12(in Chinese).

[4] SUN Qiuju, LI Jiateng, YANG Yunlu, et al. Development strategies of power grid companies under energy internet and electricity policy reforms[J]. Guangdong Electric Power, 2020, 33(2): 71-77(in Chinese).

[5] Distl B, Hossmann T. Privacy in opportunistic network contact graphs[C]//Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014. IEEE, 2014: 1-3.

[6] FENG Jijia. Implementation and research of automatic line inspection of power transmission lines based on 5G UAV[J]. Electric Power Equipment Management, 2020(9): 203-204.

[7] Cho J H, Swami A, Chen R. A survey on trust management for mobile ad hoc networks[J]. IEEE communications surveys & tutorials, 2010, 13(4): 562-583.

[8] Golbeck J, Hendler J. Inferring binary trust relationships in web-based social networks[J]. ACM Transactions on Internet Technology (TOIT), 2006, 6(4): 497-529.

[9] Keranen, Ari. "Opportunistic network environment simulator." Special Assignment report, Helsinki University of Technology, Department of Communications and Networking (2008).

[10] Pajevic L, Karlsson G, Helgason Ó. Performance of Epidemic Content Distribution in Opportunistic Networks[C]//IFIP WG 7.3 Performance 2013 31st International Symposium on Computer Performance, Modeling, Measurements and Evaluation 2013 Student Poster Abstracts September 24-26, Vienna, Austria. 2013.

[11] Huang T K, Lee C K, Chen L J. Prophet+: An adaptive prophet-based routing protocol for opportunistic network[C]//2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE, 2010: 112-119.

[12] Spyropoulos T, Psounis K, Raghavendra C S. Spray and wait: an efficient routing scheme for intermittently connected mobile networks[C]//Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking. 2005: 252-259.