The Development Direction of Industrial Internet of Things based on 5G Communication

Xiaojin Mo*
Department of Electrical and Electronic Information
Wuhan Institute of Shipbuilding Technology
Wuhan 430050, P. R. China

*Corresponding author e-mail: kristymo@163.com

Abstract. The characteristics of 5G communication system, such as ultra-high data rate, ultra-high link capacity and ultra-low delay, are very important for the development of industrial Internet of things. The information security problem of industrial Internet of things based on 5G communication system has become a major challenge in its development process. In order to protect the industrial Internet of things system from the harm of network attack, this paper studies the information security protection technology of the industrial Internet of things under the background of 5G communication, designs and realizes the security protection strategy for the industrial Internet of things based on the analysis of the security of the industrial Internet of things based on 5G communication. The experimental results show that the industrial Internet of things classification model proposed in this paper can quickly detect the attacks and make protective responses.

Keywords: Industrial Internet, 5G communication, security

1. Introduction
With the mobile communication technology completing its fifth generation (5g) cycle, it can more and more support new scenarios with strict performance requirements. In addition to providing seamless broadband connectivity for humans, 5G systems are preparing to launch a wide range of machine type applications to advance the vision of the Internet of things [1]. In addition to defining more advanced air interface technology, 5g network will also use more programmable software networking methods, and widely use it virtualization technology in telecommunication infrastructure, functions and applications [2]. 5G network is expected to expand today's Internet of things on a large scale, which can promote cellular operation, Internet of things security and network challenges, and push the future of the Internet to the edge [3]. With the explosive growth of mobile data demand, the fifth generation mobile network will make full use of the huge spectrum resources of millimeter wave band and greatly improve the
communication capacity [4]. 5G aims to participate in and benefit from the progress of many current technologies, including large-scale intensive network, interference and mobility management, Internet of things, pervasive and social computing, mobile self-organizing network cognitive radio, world wide web, cloud computing, IPv6, etc.[5].

As an advanced wireless transmission technology in the future, 5G has great potential for the development of IIot and network-based physical manufacturing system. According to the architecture and characteristics of 5g wireless communication technology, Cheng [6] proposed an IIot architecture based on 5G, and described the implementation methods of different advanced manufacturing scenarios and manufacturing technologies under three typical application modes of 5G. Hatzivasilis [7] proposed a new hybrid protocol and development framework HY-LP for industrial Internet of things. HY-LP realizes the seamless communication between iiot sensors and actuators within and between domains, and also promotes the integration of industrial cloud. Kemppainen [8] introduced the concept of the pharmaceutical industry internet, the reference model of 5G PPP infrastructure, the reference architecture of the industrial Internet Alliance and the key manufacturing standards of the pharmaceutical industry, in order to standardize the modeling and build a dedicated industrial Internet solution for the pharmaceutical industry. The Internet of things connects billions of objects to achieve high-speed data transmission, especially information collection and processing in 5G supported industrial environment [9]. Maheshwari [10] proposes a flexible beam forming antenna architecture, which allows flexibility in data rate, coverage and scalability in an energy efficient manner. The performance advantages of the proposed FBF antenna structure are verified by simulation experiments using real 5G test bench parameters.

Industrial manufacturing process requires high reliability and stability, so the development of industrial Internet of things in 5G background requires high performance, high reliability and low delay communication system is very important. This paper constructs a traffic analysis model of industrial Internet of things in the background of 5G to judge whether the industrial Internet of things operates normally.

2. Method

2.1. The Development of Industrial Internet of Things and 5G

As the product of the deep integration of industrialization and informatization, the industrial Internet of things refers to the real-time monitoring, analysis and adjustment of industrial production through key technologies such as sensors, communication, big data storage and analysis, so as to achieve the goal of optimizing resource allocation and improving production efficiency. The implementation of industrial Internet of things generally includes three levels:

1) Sensing layer

Collect industrial data with various sensors, RFID and other intelligent sensing technologies for information acquisition, information exchange, command control and equipment monitoring and maintenance;

2) Network layer

Using communication technology in the industrial Internet of things to build a communication network in the way of wired or wireless (WiFi, Bluetooth, IOT, etc.) to exchange information in various links or parts so that data and signals can be transmitted in real time and accurately.

3) Application layer

It uses data processing and analysis technology such as cloud computing to deeply mine and utilize these multi-source heterogeneous data, so as to meet the needs of various aspects of production, industry and monitoring, and then realize the management and optimization of industrial processes.
With the rapid development of wireless communication technology in recent years, wireless communication technology is more and more important in promoting the development of industrial Internet of things. Compared with the fourth generation mobile communication technology, 5G technology improves the peak rate, experience rate, connection number, low-delay, high-reliability, high-frequency spectrum efficiency and low power consumption. The fifth generation mobile communication technology has been standardized and is about to enter the stage of commercialization. In order to achieve flexible, efficient, QoS and energy aware solutions, the fifth generation mobile network is introduced to serve multiple heterogeneous devices, so that it is closer to the vision of sustainable circular economy. The low time delay of 5G technology ensures the requirement of real-time monitoring and control in the industrial field, and the high reliable network quality ensures the stability of the industrial system.

2.2. Security of Industrial Internet of Things Based on 5G Communication
The application of the industrial Internet of things has been limited to the data collection and display on the surface and some management functions extended from it. It is difficult to involve the control of the industrial system and other core areas. 5G communication system design adopts a top-down method, first defining the future application scenarios, then abstracting the technical requirements from the scenarios, then finding solutions according to each specific demand, and developing specific solutions. For the industrial field, with the popularization and application of the Internet of things, the means of illegal attacks on the network and communication are increasing. Some attacks against the Internet and industrial control network have gradually become the main security threats of the industrial Internet of things system.

1) Based on the security threat of data acquisition layer
Through breaking through the weak link of terminal equipment and the characteristics of interconnection between nodes, the illegal code value can be put into the normal data flow or the data flow can be extracted and cracked to get the authentication information, tamper with the hardware and software configuration of terminal equipment, so that the terminal equipment becomes a zombie node.

2) Security threat based on data transmission layer
The biggest security risk of the data transmission layer of the industrial Internet of things is the security vulnerability of the Internet of things communication protocol. The protocol of Internet of things is faced with many uncertain factors, so it is difficult to guarantee the security performance. As the most widely used protocol in the Internet of things, MQTT protocol lacks communication data encryption and device identity authentication.

3) Security threats based on data processing layer
The data processing layer of the industrial Internet of things is generally composed of the cloud platform of the Internet of things which provides computing and storage data services, and carries out operations such as synthesis, analysis and sorting of the collected data. It is easy to bypass the firewall detection if the forged packets conform to the protocol and access control rules, so we need to take real-time full flow analysis method to prevent such attacks.

2.3. Anomaly Traffic Detection of Internet of Things Based on Naive Bayesian Classifier
The types and type flags of the control messages in the communication process have certain statistical rules for the MQTT protocol used in the industrial Internet of things. Therefore, the traffic analysis model is constructed by collecting MQTT traffic selection classification algorithm to determine whether the industrial Internet of things system is in normal operation or under high-level persistent attack. Train the model according to the traffic data, and then use the trained traffic analysis model to detect the real-time abnormal behavior of the traffic.

1) Preparation stage
Select appropriate characteristic attributes for classification items according to the actual situation. To classify the identified feature attributes, classify some of the items to be classified, and train the classifier as the training samples. The selection, partition and quality of the training samples will have a great impact on the classification accuracy of the classifier. The category collection of abnormal traffic detection for the Internet of things includes two categories: normal traffic and abnormal traffic. The division of characteristic attributes requires the selection of protocol characteristic attributes. The key is that the selected protocol characteristic attributes should be able to contain the attack characteristics of abnormal traffic as much as possible. This stage can be described as follows: assuming that the number of characteristic attributes is m, 

\[ x = \{a_1, a_2, \ldots, a_n\} \] is an item to be classified, 
\[ a_i (i = 1, 2, \ldots, m) \] is a characteristic property of X; 
then C = \{y_1, y_2, \ldots, y_n\} is divided into a set of categories.

2) **Classifier Classifier training stage**

This stage is mainly to preprocess the training samples according to the characteristics provided in the preparation stage. In the abnormal traffic detection of the Internet of things, the samples used for training should include both normal and abnormal traffic, and calculate the probability of normal traffic and abnormal traffic 

\[ P(y_i), i = 1, 2, \ldots, n \]

and the conditional probabilities 

\[ P(a_1 | y_i), P(a_2 | y_i), \ldots, P(a_m | y_i), i = 1, 2, \ldots, n \]

3) **Classifier application stage**

According to the results of the classifier training phase, the corresponding feature attributes are extracted for the communication packets to be detected as the items to be classified, and then input to the trained classifier to get the detection results. The characteristic attribute of the item to be classified is the input, and the output is the recognition rate of each category of the item to be classified.

### 3. Construction Industrial Internet of Things Security Protection Strategy Based On 5G

In order to protect the information security of the communication process of the industrial Internet of things in 5G environment and prevent the attack of forged packets, this paper constructs an anomaly detection model based on Naive Bayes to detect and classify the real-time MQTT protocol traffic.

1) **Feature attribute selection of MQTT protocol based on industrial Internet of things**

For each MQTT packet, the control message type (characteristic attribute \( x_1 \)) and the flag bit (characteristic attribute \( x_2 \)) of the specified control message type are extracted to obtain each characteristic attribute vector 

\[ X_i = [x_1^i, x_2^i], i = 1, 2, 3, \ldots, N \]

represent the values of the characteristic properties \( x_1^i \) and \( x_2^i \) of the ith packet respectively.

2) **Data preprocessing of MQTT training samples**

We can get the sample set of eigenvector. After extracting the eigenvector of MQTT data stream, before building a naive Bayesian classifier detection model, we need to preprocess the feature vector to get the parameters of naive Bayesian classifier. Data preprocessing process Define set 

\[ M = \{(X_1, Y_1), (X_2, Y_2), \ldots, (X_n, Y_n)\}, n = 1, 2, 3, \ldots, N \]

For each feature vector, if the corresponding packet belongs to the normal flow, set identifier \( Y_i = 1 \); if the corresponding packet belongs to the abnormal flow, set identifier \( Y_i = 0 \). Count the probability of the occurrence of the normal feature vector and the abnormal feature vector in set M, the probability of the occurrence of normal and abnormal eigenvectors in statistical set M is \( p (y = 1) \) and \( p (y = 0) \). For the normal characteristic attribute vector in set M, the conditional probability of different values of characteristic attribute \( x_1 \) is calculated according to formula 1, the value
indicates the specific value of the characteristic attribute, which indicates the number of control message types:
indicates the number of control message types:

\[ P(x_1 = 1|Y = 1) = \frac{\sum_{i=1}^{N} I(x_1 = j, Y_1 = 1) + \lambda}{\sum_{i=1}^{N} I(Y_1 = 1) + \lambda s_1} \]  

(1)

The conditional probability of different values of characteristic attribute \( x_2 \) is calculated according to formula 2:

\[ P(x_2 = 1|Y = 1) = \frac{\sum_{i=1}^{N} I(x_2 = k, Y_1 = 1) + \lambda}{\sum_{i=1}^{N} I(Y_1 = 1) + \lambda s_2} \]  

(2)

Where \( \lambda \) is usually 1, \( j \) represents the specific value of the characteristic attribute \( 1, 2, 3, \ldots, s_1 \), \( s_2 \) refers to the number of control message type flag bits, the frequency of MQTT’s two characteristic attributes is calculated under the condition of normal traffic and abnormal traffic, which provides the necessary parameters for building naive Bayesian classification model.

3) classification

Input the items to be classified into naive Bayesian classification model that has completed training, and get the classification prediction results of the items to be classified. If \( P \) (normal) > \( P \) (abnormal), it is determined that the MQTT message is normal traffic processing; if \( P \) (abnormal) > \( P \) (normal), it is determined that the MQTT message is abnormal traffic processing.

4. Test and Analysis of Building Security Protection Module of Industrial Internet of Things

483 MQTT control message samples are selected to train naive Bayesian classification model. In this paper, including 292 normal control message samples and 191 abnormal control message samples. 321 message samples are selected as the control messages to be detected, including 179 normal control messages and 142 abnormal control messages. The trained Bayesian classification model is used to test the detection data, and the quality of naive Bayesian classifier is evaluated by three indicators:

1) Classification accuracy: the ratio of correctly classified samples to all classified samples,

2) False alarm rate: the ratio of abnormal samples to all classified samples,

3) Missing report rate: the classifier classifies abnormal samples as the ratio of normal samples to all classified samples.

4.1. Test Results

Three cases are selected to use naive Bayesian classification model for training in this experiment, and then use these trained models to classify another 321 data to be detected, and calculate the correct number of classification, the number of classification false alarms and the number of classification false alarms, the results are shown in Table I.

| Feature attribute | Total data to be tested | Correct quantity by classification | Number of classified false positives | Number of missing reports |
|-------------------|-------------------------|----------------------------------|-------------------------------------|--------------------------|
| Type of control message | 321 | 278 | 31 | 12 |
| Flag bit of control message | 321 | 254 | 45 | 22 |
| Type of control message and Flag bit of control message | 321 | 297 | 18 | 6 |
4.2. Analysis of Experimental Results

When selecting different feature attributes for classifier training, the classification accuracy, false alarm rate and false alarm rate of different classifiers are shown in Figure 1.

![Figure 1. Classification accuracy, false rate and missing rate with different feature attributes](image)

When only MQTT message type is selected as the characteristic attribute or only control message type flag bit is selected as the characteristic attribute, with high false alarm rate and high false alarm rate is 86.6% and 79.19% respectively according to figure 1; when MQTT control message type and control message type flag bit are selected as the characteristic attribute, the classification accuracy of naive Bayesian classifier is increased to 91.3%, with false alarm rate and false alarm rate of classification is also down a lot. According to the above test results, the anomaly traffic detection model based on Naive Bayes can effectively detect and protect the data traffic of MQTT communication in real-time.

5. Conclusion

With the continuous intelligent upgrading of industry, the demand of industrial Internet of things for broadband communication will become bigger and bigger. The bandwidth, network quality of service, delay and location of 5G communication system can meet the highest demand of industrial Internet of things. This paper tests and analyzes the security protection module of industrial Internet of things system based on 5G high-performance communication network, and designs an abnormal traffic detection module of MQTT protocol based on Naive Bayesian classification model to detect deceptive packet attacks. The experimental results show that the classification model designed in this paper has good protection effect and can quickly detect all kinds of attacks and make protective response to protect the security of industrial Internet of things.

References

[1] Galinina, O., Andreev, S., Komarov, M., & Maltseva, S. (2017). Leveraging heterogeneous device connectivity in a converged 5G-IoT ecosystem. Computer Networks, 128, 123-132.
[2] Hu, Y. C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2015). Mobile edge computing—A key technology towards 5G. ETSI white paper, 11(11), 1-16.

[3] Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1-9.

[4] Niu, Y., Li, Y., Jin, D., Su, L., & Vasilakos, A. V. (2015). A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges. Wireless networks, 21(8), 2657-2676.

[5] Hu, L., Tian, D., & Lin, K. (2018). Cognitive Industrial Internet of Things. Mobile Networks and Applications, 23(6), 1607-1609.

[6] Cheng, J., Chen, W., Tao, F., & Lin, C. L. (2018). Industrial IoT in 5G environment towards smart manufacturing. Journal of Industrial Information Integration, 10, 10-19.

[7] Hatzivasilis, G., Fysarakis, K., Soultatos, O., Askoxylakis, I., Papaefstathiou, I., & Demetriou, G. (2018). The industrial internet of things as an enabler for a circular economy Hy-LP: a Novel IIoT protocol, evaluated on a wind park’s SDN/NFV-enabled 5G industrial network. Computer Communications, 119, 127-137.

[8] Kemppainen, P. (2016). Pharma Industrial Internet: A Reference Model Based on 5G Public Private Partnership Infrastructure, Industrial Internet Consortium Reference Architecture and Pharma Industry Standards. Nordic and Baltic Journal of Information and Communications Technologies, 2016(1), 141-162.

[9] Mistry, I., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mechanical Systems and Signal Processing, 135, 106382.

[10] Maheshwari, M. K., Agiwal, M., Saxena, N., & Roy, A. (2019). Flexible Beamforming in 5G Wireless for Internet of Things. IETE Technical Review, 36(1), 3-16.