

Generative Adversarial Networks Based Industrial Protocol Construction in the Fog Computing

Chu Lu, Hong Liu

School of Computer Science and Software Engineering,
East China Normal University, China
Email: luchu1993@163.com, liuhongler@ieee.org

Abstract—Industrial protocols are critical communication elements for networking components in industrial applications, and plays core rule for security audit and anomalous detection. The emerging of fog computing paradigm makes that intelligence moves down to the industrial devices for enhanced local computational capability. In this work, deep convolutional generative adversarial networks (GAN) is applied for designing industrial protocol construction scheme, in which a discriminator and a generator are respectively established to achieve collaborative training and optimization. Siemens S7 protocol payloads are transformed into gray scale images for texture feature extraction, and a data set of industrial protocols are adopted for implementation. The adversarial training model could be uploaded in the industrial cloudlets, and the proposed protocol construction scheme will launch a perspective for establishing honeypots or honeynets in the fog computing.

I. INTRODUCTION

Industrial protocols are particularly critical communication elements for industrial networking components, and play core rule for data audit, traffic monitoring, and anomalous detection [1]. Traditional protocol analysis mainly depends on human's experiences and protocol features. While, this process is quiet time consuming, and is invalid for the unknown protocol identification. It is necessary to apply artificial intelligence to address security issues in industrial applications. Meanwhile, the emerging fog computing paradigm makes that ubiquitous intelligence moves down to the industrial devices for enhanced local computational capability [2], [3]. It makes that artificial intelligence algorithms could be invoked and executed based on the distributed system resources in the fog computing.

In industrial applications, exiting security works are mainly classified into three categories:

- *Boundary protection*: Physical and logical isolation technologies such as industrial gateway, gatekeeper, and firewall, are designed for boundary protection. Once an attacker crosses the boundary, the inside industrial systems will be exposed to the attacks.
- *Defense in depth*: Detection technologies are deployed for integration to achieve cooperative defence strategies. National Institute of Standards and Technology (NIST) published the special publication 800-82 "Guide to Industrial Control Systems (ICS) Security" for supervising industrial applications [4]. False data injection attacks are particularly considered for industrial systems [5].

- *Active defence*: Due to advanced persistent threats becoming severe, security protection trends to be transformed from passive defence to active defence against increasing attacks. Note that the possible attacks should be captured based on simulate honeypots or honeynets for data analysis, and unknown attacks should also be considered [6].

The honeypots based active defence will play an important role by distributed infrastructures, for which the fog computing is available to adopt a substantial amount of resources for functional implementation [7]. For instance, fake automation components and industrial protocols could be configured with vulnerable services in an industrial control system. An attacker may waste time for performing malicious attacks, and this time could be used to block or defend the ongoing attackers. Moreover, the honeypots are applied to learn the attacker's malicious behaviors for exploiting the zero-day attacks, and for catching system breaches [8], [9]. Here, protocol construction is indispensable for the active defense in the fog computing based industrial applications. While, it is not practical for deploying the real industrial protocols in the honeypots, and it is required to create several high-quality simulated industrial protocols instead of simulating static protocol flows with low interactions.

In order to achieve active defense, we first obtain features of industrial protocols, and further realize protocol construction. An attractive artificial intelligence algorithm, called generative adversarial networks (GAN), is applied for industrial protocol construction [10]. The GAN is originally designed for image processing, involving a generator model and a discriminator model under an adversarial training model. It is designed for estimating potential distribution of real data samples, and generating several samples ("realistic-looking data") according to the distribution. Here, a *generator* is to create data samples, a *discriminator* is to classify the samples as real or fake, and both generator and discriminator train each other to achieve cooperative training. The GAN could be applied for cooperative training on industrial protocol identification and construction, the created protocols will be realistic-looking data compared with the real protocols.

In this work, we address security issues in the fog computing based industrial applications, and propose an industrial protocol construction scheme to enhance the active defense. The main contributions include three aspects:

- Protocol identification and protocol construction are jointly considered to achieve active defense, and cooperative and adversarial security model is established for the fog computing based industrial applications.
- Industrial protocol flow payloads are transformed into gray scale images, and the Gabor filter is applied for industrial protocol texture feature extraction, which makes that the protocol flow payloads are regarded as an image for flexible processing.
- A deep convolutional GAN model is established for industrial protocol construction, and a discriminator and a generator are trained for automatic feature learning. The constructed protocols improve the discriminant ability for protocol identification.

The remainder of the work is organized as follows. Section II introduces the current works. Section III presents the proposed system model of the fog computing based industrial control systems. Section IV and Section V present a deep convolutional GAN based industrial protocol construction scheme and implementation. Finally, Section VI draws a conclusion.

II. RELATED WORKS

Most studies focus on protocol identification as an important aspect of passive defense, and there is less works on protocol construction to achieve active defense.

Wang [11] proposed an artificial neural network (ANN) and deep learning based traffic identification scheme for automatic feature learning. Stacked auto-encoder is established for learning protocol features in different depths. It enhances the unknown protocol identification, and could be applied for feature learning and anomalous detection.

Yun *et. al.* [12] proposed a semantics aware traffic classification scheme for automated protocol identification to support network measurement, network monitoring, and malware activities detection. It regards protocols as language interactions between two processes, and applies natural language processing to formalize the protocol traces. ProDecoder is proposed for analyzing unknown protocols.

Wang *et. al.* [14] identified network packet forwarding to propose a packet behavior identification scheme based on access point classifier. In this work, the classifier is designed according to an atomic predicates, and is presented as a control tool for identifying packet behavior. It is available for packet behavior identification for protocol flow verification, attack detection, and network fault localization.

The current works mainly apply artificial intelligence algorithms for addressing unknown and encrypted traffic analysis, and aim to enhance protocol identification in ubiquitous applications. While, protocol construction is more significative for support the active defense, and also introduces the artificial intelligence algorithms to generate the realistic-looking data. Here, a deep convolutional GAN is established for protocol construction, in which both protocol identification and protocol construction are considered to achieve collaborative training and optimization.

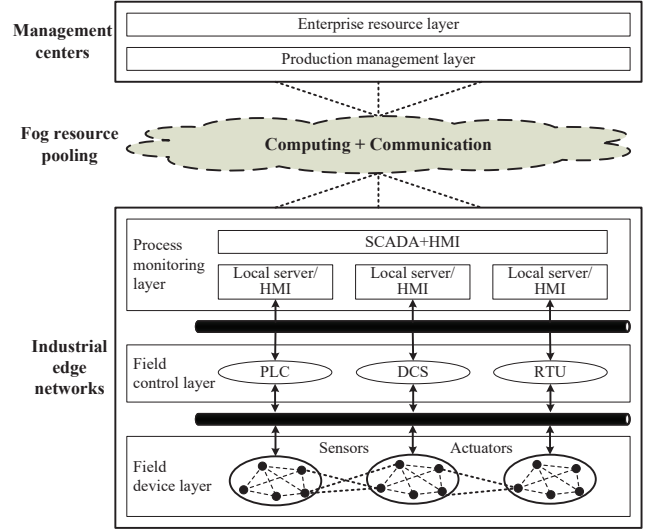


Fig. 1. System model of the fog computing based industrial control systems.

III. SYSTEM MODEL

Figure 1 illustrates the proposed system model of the fog computing based industrial control systems, which covers several types of control elements and associated instrumentation for industrial process control. Fog computing is regarded as the local cloudlets for emphasizing proximity to terminals for function interactions. This system model realizes to establish a dense geographical distribution and local resource pooling.

There are three main system components as follows:

- **Industrial edge networks:** Industrial edge networks include three layers: field device layer, field control layer, and process monitoring layer. In the field device layer, sensors and actuators are deployed for production process data collection, and production process operation. In the field control layer, control functions are performed by control units such as programmable logic controller (PLC) and distributed control systems (DCS). In the process monitoring layer, supervisory control and data acquisition (SCADA) systems are applied to obtain and monitor the industrial processing parameters. Engineer stations, operator stations, and OPC servers are applied for industrial process monitoring.
- **Fog resource pooling:** Fog computing provides distributed infrastructure, platform, software services to support convenient computing requirements. It enables local services lay on edge networks instead of uploading them to the remote servers, and it is to extend cloud computing to the edge networks [15]. The aggregated resources could apply more intelligent algorithms for enhanced functions. Fog resource pooling is a medium weight and intermediate level to establish interconnections between industrial edge networks and management center.
- **Management centers:** Management centers include production management layer and enterprise resource layer. The former refers to manufacturing execution systems

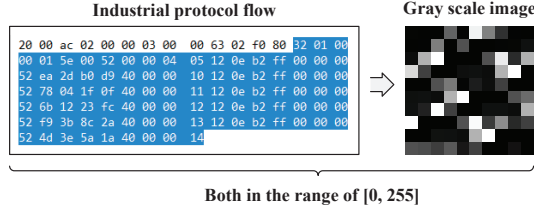


Fig. 2. The transformed gray scale image of the industrial protocols.

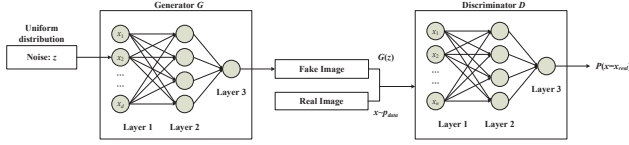


Fig. 3. The GAN adversarial model.

(MES) providing management functions such as manufacturing data management, scheduling management, and production management. The later refers to that enterprise resources planning (ERP) providing decision-making services. Management centers are similar to other computer systems to achieve supervision and scheduling.

IV. INDUSTRIAL PROTOCOL CONSTRUCTION SCHEME

A. GAN Adversarial Model Training

In the GAN model, there is a generator G and a discriminator D . G refers to the data distribution, and D is defined to estimate the probability of a sample coming from the training data rather than G . Define that the inputs are x and random noise variables n , and functions $D(\cdot)$ and $G(\cdot)$ are applied to represent D and G . $G(z)$ refers to that a sample is generated by the generator G , and satisfies the distribution of real industrial protocol feature x .

Towards the discriminator D , it performs identification on the inputs from either the real data x or the fake samples $G(z)$. If the input data is from x , D will remark it as true. If the input data is from $G(z)$, D will remark it as false. Here, D is designed for performing correct identification of the data source, and G is designed to improve the computed value $D(G(z))$ to be converged with $D(x)$.

The GAN adversarial model is shown in Figure 3, the adversarial optimization is achieved along with the performance improvement of both D and G . It is expected that D 's discrimination ability will achieve a high level but could not discriminate the data source with high precision, and G 's data construction ability will also achieve a high level with extremely similarity with the distribution of real data [10]. During feature learning and training, G and D are improved along with the generated data and the training data being indistinguishable. D and G satisfy the following relationship.

During the adversarial training, there are two data sources: the real data distribution p_{data} , and the generated data distribution $p_g(x)$. In order to train D for maximizing the probability of correctly determining the training examples and samples

from G . Simultaneously, G is trained to minimize $\log(1 - D(G(n)))$, and the minimax game is to obtain $V(G, D)$.

$$\min_G \max_D V(G, D) = \mathbb{E}_{x \sim p_{data}(x)} [\log D(x)] + \mathbb{E}_{n \sim p_n(n)} [\log D(G(N))]$$

Here, $\mathbb{E}(\cdot)$ is the expectation, p_{data} is the real data distribution for x is sampled from p_{data} . $p_z(z)$ is the prior distribution. $G(z, \theta_g)$ is a data space, in which G is a differentiable function represented by a multi-layer perceptron with parameters θ_g . $D(x, \cdot)$ is a second multi-layer perceptron with a single scalar as its output. $D(x)$ refers to the probability that x is from the real data rather than p_g . Given a generator G , the optimal discriminator D is as follows:

$$D'_G(x) = \frac{p_{data}(x)}{p_{data}(x) + p_g(x)}$$

The discriminator D is allowed to achieve G , and p_g is returned for optimization to realize the convergence p_g and p_{data} . Based on the GAN model, the adversarial model parameters are trained for generating realistic-looking protocol data.

B. Deep Convolutional GAN Based Protocol Construction

The unsupervised representation learning is achieved based the GAN and convolutional networks (CNNs).

- For a discriminator D , the pooling layers could be replaced with the strided convolutions;
- For a generator G , the pooling layers could be replaced with the fractional-strided convolutions.

The generator G applies convolution for the faked images generation. The discriminator D simultaneously inputs the real data transformed by the real industrial protocols x_{real} , and the generated data x_{fake} .

During the model training, images obtained by the industrial protocols are scaled to the range of tanh activation function $[-1, 1]$. The mini-batch stochastic gradient descent is applied for model training based on a size of 100. No maxpooling operation is performed, upsampling with fractionally-strided (stride=2) convolution is performed.

The discriminator is trained for image identification with enhanced performance, and the generator is trained for image construction.

V. IMPLEMENTATION

The data set of industrial protocols is from the ICS Lab [21], which covers the PLCs, RTUs, servers, industrial equipment, and these devices are available for supporting the testing task.

Siemens S7 protocol (i.e., S7comm) is applied for analysis. S7comm is a proprietary protocol that runs between the PLCs of the Siemens S7-300/400 family [22]. There are 106421 items of S7comm protocol payloads are imaged for adversarial model training. The main deploy environment includes:

Job and *ACK_Data* are two typical messages in the S7comm protocol. A message pair of *Job* and *Ack_Data* is performed. *Job* and *Ack_Data* are transmitted at the beginning of each

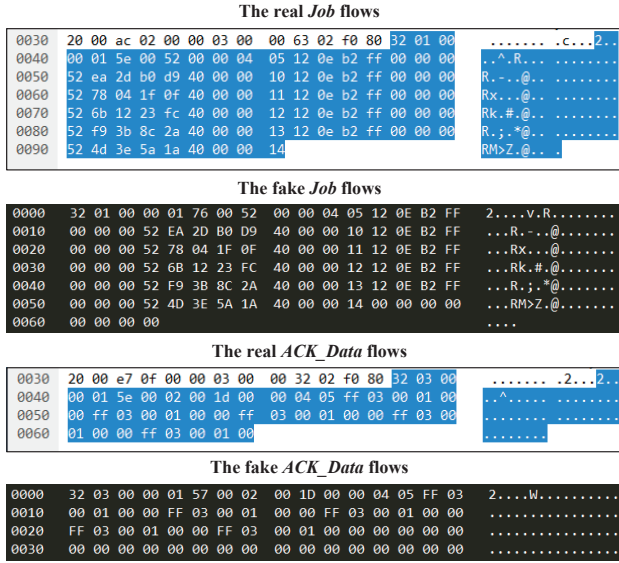


Fig. 4. The comparison between the real and fake protocol flows.

session for negotiating the size of the *Ack_Data* queues and the max protocol data unit (PDU) length. The length of the *Ack_Data* queues determine the number of parallel jobs that can be initiated simultaneously without acknowledgement.

Here, a generative network is to transform the real S7comm protocol samples into adversarial samples. The adversarial training neural network is able to result in nearly 0 true positive rate on both the real data distribution p_{data} , and the generated data distribution $p_g(x)$.

The deep convolutional GAN adversarial model is simultaneously trained for cooperative optimization. The generator G will generate the fake S7comm protocol payloads, and the discriminator D will be unable to differentiate the real S7comm protocol payloads and the generated fake samples (i.e., $D(x) = \frac{1}{2}$). Moreover, both G and D have sufficient computing capacity based on the fog resource pooling, it will obtain a balance point at which both cannot improve since p_g equals p_{data} .

The comparison between the real and fake protocol flows is shown in Figure 4. It indicates that the generated fake samples have a high similarity, which could not be distinguished by the discriminator or other entities.

VI. CONCLUSION

This article applies deep convolutional GAN for achieving realistic-looking industrial protocol construction, and Siemens S7 protocol flow payloads are transformed into gray scale images for processing. A discriminator and a generator are respectively established to achieve collaborative training and optimization. The adversarial training model could be applied in the distributed cloudlets for establishing honeypots with active defence requirements. It indicates that artificial intelligence algorithms such as GAN and CNN could be invoked and executed to support the distributed and ubiquitous intelligence for the fog computing based industrial control systems.

ACKNOWLEDGMENT

This work is funded by National Natural Science Foundation of China (61601129), and National Key R&D Program of China (2017YFB0802302, 2017YFB0801701). This work is partially supported by Shanghai Science and Technology Commission Program (No. 18511105700).

REFERENCES

- [1] A. Amrein, V. Angeletti, A. Beitelret, and et al., "Security Intelligence for Industrial Control Systems," *IBM Journal of Research and Development*, vol. 60, no. 4, pp. 13:1-13:12, 2016.
- [2] S. Zahra, M. Alam, Q. Javaid, and et al., "Fog Computing Over IoT: A Secure Deployment and Formal Verification," *IEEE Access*, 2017.
- [3] C. Mouradian, D. Naboulsi, S. Yangu, and et al., "A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges," *IEEE Communications Surveys & Tutorials*, 2017.
- [4] NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- [5] R. Deng, G. Xiao, and R. Lu, "Defending Against False Data Injection Attacks on Power System State Estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198-207, 2017.
- [6] J. Yang, C. Zhou, S. Yang, H. Xu and B. Hu, "Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems," *IEEE Transactions on Industrial Electronics*, 2018.
- [7] F. Kargl, R. W. van der Heijden, H. K?nig, A. Valdes and M. C. Dacier, "Insights on the Security and Dependability of Industrial Control Systems," *IEEE Security & Privacy*, vol. 12, no. 6, pp. 75-78, 2014.
- [8] S. Abe, Y. Tanaka, Y. Uchida, and S. Horata, "Tracking Attack Sources Based on Traceback Honeypot for ICS Network," *2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, Kanazawa, Japan, pp. 717-723, 2017.
- [9] W. Fan, Z. Du, D. Fernández and V. A. Villagrà, "Enabling an Anatomic View to Investigate Honeypot Systems: A Survey," *IEEE Systems Journal*, 2017.
- [10] I. Goodfellow, J. Pouget-Abadie, M. Mirza, and et al. "Generative Adversarial Nets," *Advances in Neural Information Processing Systems 27 (NIPS 2014)*, Montreal, Quebec, Canada, pp. 2672-2680, 2014.
- [11] Z. Wang, "Applications of Deep Learning on Traffic Identification," *Black Hat USA 2015*, Las Vegas, US, 2015.
- [12] X. Yun, Y. Wang, Y. Zhang, and Y. Zhou, "A Semantics-Aware Approach to the Automated Network Protocol Identification," in *IEEE/ACM Transactions on Networking*, vol. 24, no. 1, pp. 583-595, 2016.
- [13] V. F. Taylor, R. Spolaor, M. Conti, and I. Martinovic, "Robust Smartphone App Identification via Encrypted Network Traffic Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 63-78, 2018.
- [14] H. Wang, C. Qian, Y. Yu, H. Yang, and S. S. Lam, "Practical Network-Wide Packet Behavior Identification by AP Classifier," *IEEE/ACM Transactions on Networking*, vol. 25, no. 5, pp. 2886-2899, 2017.
- [15] J. Ren, H. Guo, C. Xu, and Y. Zhang, "Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing," *IEEE Network*, vol. 31, no. 5, pp. 96-105, 2017.
- [16] A. K. Jain, and F. Farokhnia, "Unsupervised Texture Segmentation Using Gabor Filters," *IEEE International Conference on Systems, Man, and Cybernetics Conference Proceedings*, Los Angeles, CA, pp. 14-19, 1990.
- [17] S. E. Grigorescu, N. Petkov, and P. Kruijinga, "Comparison of texture features based on Gabor filters," *IEEE Transactions on Image Processing*, vol. 11, no. 10, pp. 1160-1167, 2002.
- [18] Y. Chen, L. Zhu, P. Ghamisi, X. Jia, G. Li, and L. Tang, "Hyperspectral Images Classification With Gabor Filtering and Convolutional Neural Network," *IEEE Geoscience and Remote Sensing Letters*, pp. 1-5, 2018.
- [19] N. Onizawa, K. Matsumiya, W. J. Gross and T. Hanyu, "Accuracy/energy-flexible stochastic configurable 2D Gabor filter with instant-on capability," *ESSCIRC 2017 - 43rd IEEE European Solid State Circuits Conference*, Leuven, pp. 43-46, 2017.
- [20] Web-enabled image processing operators, <http://www.cs.rug.nl/~imaging/>
- [21] Capture Files from 4SICS Geek Lounge, <http://www.netresec.com/?page=PCAP4SICS>
- [22] S7 Communication (S7comm), <https://wiki.wireshark.org/S7comm>