OTG: A Gateway for Cybersecurity in the Context of OPC UA PubSub Pattern

Tianyu bu*, Jiahao Liu, Jinfeng Huang, Zhigang Sun
College of Computer, National University of Defense Technology, Changsha 410073, China
876959267@qq.com
butianyu14@nudt.edu.cn

Abstract. Under the background of industrial intelligence, OPC UA PubSub mode is strongly supported by Industry 4.0 as a protocol designed to meet the communication requirements of industrial control level. With the gradual opening of industrial control network, the PubSub security model in OPC UA protocol alone cannot meet the new security requirements under the background of OT and IT integration. According to the specification, we analyze the possible threats, impacts and countermeasures that PubSub may face in OPC UA deployment environment, and emphasized that PubSub security model is difficult to protect resource-constrained industrial field equipment from the harm caused by DoS and other attacks. In view of the limited resources of industrial control network, this paper proposes that OTG gateway provides protection for PubSub service. Compared with traditional security gateway, OTG gateway can greatly reduce the consumption of industrial control network resources by network attacks. In addition, according to the characteristics of PubSub protocol, a DoS detection algorithm for this architecture is proposed. Compared with the traditional DoS detection algorithm, it has better applicability to PubSub protocol and can detect DoS attacks more accurately to reduce the impact on device performance. Experiments show that the DoS detection algorithm has 100% accuracy and 0.13% false positive rate, and can detect DoS attacks faster than the traditional detection algorithm.

1. Introduction

OPC UA (Unified Architecture) is the next generation of OPC standards by providing a complete, secure, and reliable cross-platform Architecture to capture real-time and historical data and time. The OPC UA PubSub specification defines message-oriented middleware, a communication pattern that supports two message-oriented middleware patterns, the agent-based pattern and the agentless pattern. Proxy-based mode is usually used in the public Internet, while proxy-based mode is limited to multicast and can only be used in the LAN. Therefore, proxy-based mode is better applicable to the closed industrial control network. The OPC Foundation proposes a security model in the second part of the OPC UA protocol, including the security model for the newly extended PubSub pattern. This model analyzes the security of PubSub communication mode under OPC UA deployment environment, illustrates the security threats and impacts PubSub faces, and proposes appropriate reconciliation methods. The implementation of PubSub model security mechanism mainly depends on message encryption and decryption and signature. For attacks that cannot be resisted through encryption and decryption and signature, the security model gives suggestions for detecting UADP headers.
However, under the background of OT and IT integration, industrial control network is gradually becoming more open, and the possibility of invading industrial control layer equipment through external network is greatly increased. Whether it is an external intrusion or an internal malicious or faulty operation, you can expand the attack on the device layer Subscriber with the help of the Publisher of the control layer. The proposed reconciliation method in the security model cannot defend against the attack from legal Publisher, nor can it prevent the attack from consuming resources to the industrial control network and field equipment with limited resources and the corresponding performance impact.

In this paper, we propose OTG, a soft-hard coordinated security gateway framework, and a series of mechanisms to protect OPC UA PubSub service security. We set OTG between the industrial control layer and the industrial equipment layer, and monitored PubSub communication message to achieve the purpose of security protection. Experimental results show that OTG can provide effective security protection with minimal impact on the performance of OPC UA PubSub. At the same time, we proposed a DoS detection algorithm for OPC UA PubSub mode. Experimental results show that the algorithm can detect and block DoS attacks at an early stage while ensuring high accuracy and low false positive rate, so as to minimize the performance impact of DoS attacks.

2. Related Research

Since the OPC Foundation released the OPC UA PubSub specification in early 2018, there is still a lack of complete implementation, and the research on its security in academia and industry is not comprehensive enough. Julien[7] et al. assessed the impact of attacks on OPC UA applications in the context of Industry 4.0. Based on the OPC UA specification, they identified possible threats and countermeasures for using OPC UA applications in an industry 4.0 scenario, including Client/Server mode and Publish/Subscribe mode. In an industry 4.0 environment, they modeled the security threats mentioned in the specification, highlighting the vulnerability of OPC UA applications implemented on the actual test bed to eavesdropping and message flooding attacks. However, they did not fully analyze the security threats faced by OPC UA PubSub mode, nor did they propose corresponding countermeasures.

Dimitris et al. [8] analyzed the vulnerabilities in the Industry 4.0 network paradigm and listed potential attacks that could be used to destroy network integrity.

In addition, a number of standards and protocols that may support integration are listed, including the OPC UA protocol. They used an example of an iot system in production to describe how to overcome these security threats, but did not provide countermeasures. These security threats will also appear in OPC UA PubSub mode, but the attack characteristics of this mode will be different, and countermeasures should be formulated efficiently according to the attack characteristics.

Charles[9] et al. studied DoS attacks on untrusted clients in encrypted OPC UA network. Based on the information security threats analyzed by BSI, denial-of-service (DoS) attacks in encrypted communication were emphatically analyzed, and different DoS attacks in OPC UA environment were described and analyzed. They generated data related to normal behavior and different DoS attacks in a simulated OPC UA environment, and measured CPU consumption in these different simulated scenarios. A data mining method was proposed to detect encrypted DoS attacks in OPC UA networks. Although they carried out security threat analysis for Client/Server mode and proposed DoS algorithm, they still have reference significance in PubSub mode. Even so, they do not analyze and design algorithms for the PubSub pattern.

Mudhakar et al. [10] proposed a reliable framework and a defense mechanism for EventGuard to ensure coverage of the PubSub service. EventGuard includes a set of security guard systems that can seamlessly plug into a common, content-based subsystem. They also showed a prototype implementation of EventGuard on Siena to show that EventGuard can be easily stacked on top of any content-based published-subscribe core. They made a detailed analysis of the security threats in the PubSub mode and proposed corresponding countermeasures. But EventGuard and OPC UA applications have a lot of overlap in the security model and cannot be applied to the OPC UA PubSub pattern.
3. OTG Architecture and Implement

3.1. OTG Architecture

The OTG gateway function is modular in design, and we use software defined architecture to centrally control it. On the control plane, we provide an external controller in a logical set to manage the security functions of the gateway. It provides a platform for users to manage the gateway, and the internal agent of the gateway is responsible for the control of the gateway functional modules. On the data plane, we realize efficient co-processing of software and hardware through CPU/FPGA heterogeneous resources. The gateway interface follows I2NSF standards. The communication between I2NSF User module and Security Controller module adopts the user-oriented interface, while the communication between Security Controller module and Agent module adopts the NSF-oriented interface.

As shown in Figure 1, the gateway consists of three control modules and four function modules. The control module includes an external controller, security agents, and ACL management functions. The functions of the gateway are centrally managed by an external controller through which users can issue security policies to the gateway. The security agent is responsible for sending the security rules to the corresponding module for processing. The ACL management module is responsible for issuing rules to the Pkt_ACL module of the hardware pipeline. Functional modules include software filter module, DoS detection module, timestamp module and Pkt_ACL filter module. The software filtering module includes UADP_ACL function and UADP_DPI function, which filters the messages according to the UADP header, and UADP_DPI function, which is responsible for deep packet detection of the messages. DoS detection module includes delay statistics and DoS detection function. Delay statistics is responsible for calculating the delay of the corresponding PublisherID message to calculate the threshold value of DoS detection algorithm, and DoS detection function is responsible for detecting the DoS attack based on legitimate Publish message. The timestamp module is responsible for stamping the message that has just entered the gateway. The Pkt_ACL module is responsible for filtering according to headers.

In the control plane, the user can issue a security policy to the gateway through the external controller, and the security agent receives the security policy and forwards it to the software filter module, DoS detection module or ACL management module according to the destination module. The software filter module and THE DoS detection module send the rules generated during message processing to the ACL
management module. The ACL management module uniformly issues the rules from each location to the HARDWARE’S Pkt_ACL module.

On the data plane, after entering the gateway, the message first enters the hardware pipeline. The time-stamp function stamps the message, Pkt_ACL filters the message according to the header, and the unfiltered message is forwarded by the hardware to the software for processing. The message first enters the software filtering module, and is filtered according to UADP header and UADP load. If malicious messages occur, corresponding hardware Pkt_ACL filtering rules will be generated. The filtered message enters the DoS detection module to monitor the transmission delay and DoS attack. If DoS attack occurs, corresponding hardware Pkt_ACL filtering rules will be generated. The message that passes the DoS detection will be sent to the sending port of the gateway and sent to the network.

3.2. DoS Attack Detection

The workflow of OPC UA Pub/Sub is as follows: Firstly, the OPC UA Subscriber sends the subscription request message to the OPC UA Publisher, and then the Subscriber and Publisher jointly negotiate the relevant parameters of subscription publication (including the maximum publication frequency, etc.), and finally, Publish message will be sent to the Subscriber every time the subject of the Subscriber subscription has an update Publisher. In industrial networks, there is a certain requirement for delay of industrial communication, which is usually the requirement of Publish message with upper limit of communication delay. In order to ensure the transmission requirement of OPC UA Publish message, the Subscriber and Publisher are located in the network, which distributes the transmission path of Publish message to meet the transmission upper limit requirement. The attacker makes flood attack by invading OPC UA Publisher and controlling Publisher to Publish message to the Subscriber over frequency. Assuming that the maximum publication frequency agreed by the OPC UA Publisher and the OPC UA Subscriber is $f$, the minimum release time interval of Publish message is $t$. When the Publish message arrives at the Subscriber, the gateway will actively stamp the message and save the time stamp. When the next message arrives at the gateway, the message will be timestamped first, the current message will be timestamped with the saved timestamp, and then the current message will be overwritten with the saved timestamp. The maximum $T_{max}$ and minimum $T_{min}$ transmission delay of Publish message to the Subscriber after transmission over the network is $\Delta t \geq t$. $T_{max}$ is less than or equal to the industrially required upper limit of transmission delay, and $T_{min}$ is greater than or equal to the transmission path delay (because there may be some queuing delay).

As shown in the figure 2, there should be three state elements in the finite state set $Q$ of DFA, which can be divided into safe state, critical state and attacked state. The initial state $q_0$ is safe state. The transition function $\delta$ determines the state jump based on the current state of the DFA and the value range of $\Delta t$ and $T$. When the current state is safe, if $\Delta t \geq t$, then the next state is still safe; if $\Delta t< t$, then the state that the DFA will jump to is critical. Meanwhile, perform the following operation $T = T \Delta t - (t - \Delta t)$ on $T$, if the value of $T$ is greater than $T_{max} - T_{min}$, then $T = T_{max} - T_{min}$. If $\Delta t < t$ and $T < 0$, then the next state is still underattack. Meanwhile, perform the following operation $T = T \Delta t - (t - \Delta t)$ on $T$, if the value of $T$ is greater...
than \( T_{\text{max}} \) if \( T_{\text{min}} \). Then \( T = T_{\text{max}} - T_{\text{min}} \). When the DFA jumps to the state under attack, it indicates that the Subscriber is suffering a flood attack from the OPC UA Publish mode.

4. Evaluation

![Experimental Setup](image)

As shown in the figure 3, we designed an experimental bench to evaluate the performance of the OTG security gateway. It includes a security controller, an OTG prototype system, and a network emulator. The OTG prototype and network emulator were built on the Xilinx Artix-7 FPGA, connected to the ARM Architecture A9 CPU (866MHz, single-core dual hardware threads) and PCIE. In the OTG prototype, one thread is assigned to the OS and another thread is used to run the vSFs. All links between the OTG prototype and the emulator are 1GB fiber.

We mainly tested the DoS detection algorithm for OPC UA PubSub, including the selection of algorithm threshold, accuracy rate and false alarm rate. The network emulator plays the roles of packet issuing, WAN simulation and packet receiving at the same time. Three packets are run on the WAN emulator at the same time, and each packet issuing thread has equal time interval. The first thread is the thread of DoS attack, the maximum agreed publishing frequency is 50Hz, the publishing frequency in the case of DoS attack will exceed 50Hz, and the PublisherID is 1. The second and third threads are normal published experimental threads, with the agreed maximum publishing frequency of 40Hz and 60Hz, and the PublisherID of 2 and 3 respectively. We use the network simulator to simulate the network delay, jitter and delay distribution, and the delay distribution adopted in the experiment conforms to the normal distribution.

We tested the OTG security gateway in two experimental environments. When the delay is 50ms, the agreed minimum release cycle of the measurement is 5, 10, 15, 20 and 25ms. When the delay is 100ms, the agreed minimum release cycle of the measurement is 10, 20, 30, 40 and 50ms. The contract issuing test rate is the average value of the normal release rate, 50% of the average value of the upper and lower extension, and the uniform test is conducted for 10,000 times to calculate the accuracy rate and false alarm rate.

In the first experimental environment, the selected parameters are network transmission delay of 50ms and network jitter of 30%, that is, the network transmission delay is between 35ms and 65ms. Figure 4 (1) as the thread 1 released in normal cases, 1000 times statistics obtained in the course of numerical scatterplot, choose the minimum value, also is the statistics of transport delay of the minimum and maximum transmission delay difference, it can be seen that the minimum approach to 30, is approaching the actual transmission delay differential values of minimum and maximum values. Figure 5(1) shows the accuracy rate and false alarm rate of OPC UA PubSub detection algorithm in the state of DoS attack launched by thread 1. It can be seen that the DoS detection algorithm has 100% accuracy rate and low false alarm rate.

The parameters of the second experimental environment were 100ms network transmission delay and 30% network jitter, that is, the network transmission delay is between 70ms and 130ms. Figure 4(2) as the thread 1 released in normal cases, 1000 times statistics obtained in the course of numerical scatterplot, choose the minimum value, also is the statistics of transport delay of the minimum and maximum transmission delay difference, it can be seen that the minimum approach 60, is approaching the actual transmission delay differential values of minimum and maximum values. Figure 5(2) shows the accuracy rate and false alarm rate of OPC UA PubSub detection algorithm in the state of DoS attack.
launched by thread 1. It can be seen that the DoS detection algorithm has 100% accuracy rate and low false alarm rate.

![Scatter Diagram of Δt-t in 1000 times test](image)

(a) 50ms Latency & 30% Jitter  
(b) 100ms Latency & 30% Jitter

Fig. 4 Scatter Diagram of Δt-t in 1000 times test

| Interval /ms | Accuracy | False alarm rate |
|--------------|----------|------------------|
| 5            | 100%     | 0.129%           |
| 10           | 100%     | 0.131%           |
| 15           | 100%     | 0.131%           |
| 20           | 100%     | 0.130%           |
| 25           | 100%     | 0.129%           |

(a) 50ms Latency & 30% Jitter  
(b) 100ms Latency & 30% Jitter

Fig. 5 Accuracy & False Alarm Rate of DoS Attack Detection

| Interval /ms | Accuracy | False alarm rate |
|--------------|----------|------------------|
| 10           | 100%     | 0.130%           |
| 20           | 100%     | 0.131%           |
| 30           | 100%     | 0.129%           |
| 40           | 100%     | 0.130%           |
| 50           | 100%     | 0.131%           |

5. Conclusion

Based on the results and discussions presented above, the conclusions are obtained as below. We present the design of a novel security gateway framework with SmartNIC acceleration called OTG. It provides ACL, DPI and DoS attack detection algorithm for OPC UA PubSub to protect industry control network from malicious attack. In the future, we will design a quantitative model with more detailed security functions. We believe OTG will serve as a useful platform for industrial security operators to protect.

References

[1] German Federal Office for Information Security (BSI). 2017. OPC UA Security Analysis. [Online]. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/OPCUA/OPCUA.pdf?__blob=publicationFile&v=2.

[2] Polge J, Robert J, Le Traon Y. Assessing the impact of attacks on OPC-UA applications in the Industry 4.0 era[C]//2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2019: 1-6.

[3] Mourtzis D, Angelopoulos K, Zogopoulos V. Mapping Vulnerabilities in the Industrial Internet of Things Landscape[J]. Procedia CIRP, 2019, 84: 265-270.

[4] Neu C V, Schiering I, Zorzo A. Simulating and Detecting Attacks of Untrusted Clients in OPC UA Networks[C]//Proceedings of the Third Central European Cybersecurity Conference. 2019: 1-6.

[5] Srivatsa M, Liu L. Securing publish-subscribe overlay services with eventguard [C]//Proceedings of the 12th ACM conference on Computer and communications security. 2005: 289-298.

[6] Tsien Y L, Gai R L. User Activity Based Application-Layer DoS/DDoS Attack Defense Algorithm[C]//Applied Mechanics and Materials. Trans Tech Publications Ltd, 2015, 742: 693-697.