Use of HTTP filtering devices in automated control systems based on the technology of the Industrial Internet of Things

K I Budnikov, O V Serdyukov, AV Kurochkin, RV Nestulya

Institute of Automation and Electrometry SB RAS, 1, Akad.Koptyugaave., Novosibirsk, 630090, Russia

E-mail: Budnikov@iae.nsk.su

Abstract. The use of the Industrial Internet of Things (IIoT) technology helps to increase the efficiency of the enterprise and reduce production costs. IIoT devices send large amounts of data that tied directly to production and related factors to a cloud storage. In addition, IIoT devices are used by engineering personnel through wireless devices. One of the protocols for interacting with IIoT devices is HTTP using embedded web servers. Establishing a secure HTTPS protocol connection is not always possible or justified due to its resource consumption. In this situation, to increase security, it is appropriate to apply an additional HTTP filter to regulate the access of mobile devices being used by engineering personnel to access to IIoT devices, as well as to certain features that specific devices provide over HTTP. The paper discusses HTTP filtering devices on Gridex-II hardware platform of the industrial type. The results of their bench tests with standard and improved filtering algorithms are presented.

1. Introduction
The Industrial Internet of Things (IIoT) is one of the main components of the Industry 4.0 concept. The use of this technology helps to increase the efficiency of the enterprise and reduce the cost of production [1,2]. Within its framework, the enterprise is massively digitalized with IIoT devices, which make it possible to measure various parameters with the help of sensors that relate directly to production and tied factors, including energy consumption, the state of the environment inside and outside the production room. Devices have unique identifiers on the network and transmit the collected information via communication lines to a cloud storage and data processing centers for subsequent analysis using industrial big data research technology. Processing results in the cloud contribute to decisions to improve production [3].

IIoT devices provide a large data flow to the cloud storage. In order to reduce it, edge computations are used that are a variant of distributed computing in which the data warehouse and computations approach the place where it is necessary. It improves response time and saves bandwidth [4].

Unlike the ordinary Internet of Things (IoT), industrial one is characterized by the high density of devices located in the plant floors and the need for supervisory control by engineering personnel. There is a tendency to perform this function using mobile devices, including tablets and smartphones [5].

One of the protocols being used to communicate with an IoT device is HTTP using the built-in web server. The reason why the unprotected protocol is used is the resource consumption of establishing a connection using the secure HTTPS protocol, which is not always justified [6]. On the other hand,
interacting with a client over Wi-Fi using an encrypted connection protects to a certain extent the process of exchanging information between the IIoT device and its client. As an additional security device, it is appropriate to use an HTTP filter to regulate the access of mobile devices of technical personnel to IIoT devices, as well as to those or other capabilities that these devices provide via HTTP on the pages of their sites.

Thus, the described architecture of an automated system based on technology of the Industrial Internet of Things looks as shown in Figure 1.

![Figure 1. Architecture of an automated control system based on technology of the Industrial Internet of Things using HTTP protocol.](image)

Currently, the most popular method of organizing selective access to resources via HTTP is the filtering of requests by URL. It is most balanced in relation to the advantages and disadvantages. It is based on the analysis of requests to information resources located on the same IP address. It allows authorizing or denying access to those ones of them that are necessary.

When it is used the standard filtering algorithm by URL [7,8], the user’s request that passes through the filter is intercepted and the URL of the resource being requested is extracted from it. Then, this address is searched in the lists of resources that are prohibited or vice versa allowed. The request is passed to the Internet, it reaches the server with the necessary resource, and the server returns a response with the requested information in the case of the URL address to which the call is made is allowed. Otherwise, the request is blocked by the filter.

An improved filtering algorithm with post-analysis of requests compared with the standard sequence of packet processing gives a gain in the time it takes for a user request to pass through a filtering device. It includes the time spent defining a TCP session for each packet, generating a user request from the packets, retrieving the identifier of the requested resource from the URL and checking the request for access to the requested resource from the internal lists of prohibited URLs.
According to the results of computer simulation, it was found: there is a decrease in the average waiting time for a response from a web server when passing a user request to a web resource through the emulated filtering device that worked using the post-analysis of requests to 14% compared to a device that worked in standard request analysis mode. The filter capacity increased by up to 54% [9].

To get better results using the improved algorithm, a hardware support for this method is required. The article discusses one of the options for such support along with the results of tests using the test bench. As a hardware platform for the filter, a solution based on the Gridex-II family of industrial computers of the Tornado Modular Systems company is used [10].

2. Structure of the filtration device and the model of the production subsystem.

The filtering device operating according to the standard algorithm has two equivalent channels. They pass a packet stream through the device and filter it (Figure 2).

**Figure 2.** Filter model with a standard algorithm as a part of the simulated production subsystem.

Both channels contain the following modules: the network interface (MNI), reading network packets (MPR), sorting packets (MPS), and transmitting packets (MPT). The packet analyzer (MAP) processes packets of both channels. Interaction with communication lines occurs through the modules of the network interfaces MNI1 and MNI2. The operation of the filtering device is discussed in more detail in [11]. Figure 2 shows a model of the production subsystem, which is a combination of embedded web servers in devices and their clients. They send requests to web resources located on web servers through the filtering device that controls client access to resources. The purpose of modeling is to determine the conditions for the most rapid passage of requests through the filter.

**Figure 3.** Filter model with a enhanced algorithm and hardware support as a part of the simulated production subsystem.
If the standard algorithm for the device is implemented by software on an industrial computer, then for the improved algorithm, hardware support for the filtering process is implemented as follows. The filtering device was presented as a composition of 2 logical parts. One of them is responsible for the analysis of packets, and the other one for the implementation of specialized functions of their transmission, which was assigned to the programmable switch. On the basis of an industrial computer, the packet analyzer continues to function (Figure 3). For implementation of the improved algorithm this approach creates new opportunities.

3. Gridex-II hardware platform

The presented industrial-type filtering device is a device based on the Gridex-II hardware platform, which is a development of the Gridex platform. The computer consists of a carrier card (CBCE), a processor module (SOM), and a set of expansion modules (Figure 4).

Figure 4. Gridex-II processor platform.

SOM is a system on a module - a self-contained processor device capable of functioning under the control of an operating system. IPC GRIDEX II uses COM Express Compact Type 6 SOM standard. The carrier card provides mechanical fastening of the SOM, its power supply, generation of service signals, coordination of peripheral interfaces with external switching elements and expansion of the interface composition. The electric circuits combining SOM and CBCE are formed by a set of dissimilar signals and buses in accordance with the COM Express Type 6 standard and are switched by a specialized connector - COM Express.

The execution of the processor part of the computer in the form of an independent standardized module (SOM) provides the opportunity to optimize the IPC GRIDEX II parameters in accordance with its scope without changing the design. The design of IPC GRIDEX II allows the user to make changes to the composition of internal equipment and a set of external interfaces.

The device on the Gridex-II platform has:

- passive cooling;
- standard expansion ports for installing communication adapters (RS-485/232, Ethernet, WiFi, 3G, HDD, SSD);
• 24V power supply - the basis for organizing highly reliable power supply;
• support for time synchronization according to IEEE-1588 standard;
• the ability to operate in harsh conditions at a temperature of -20 to +70 degrees C;
• sheath protection according to IP54;
• vibration resistance;
• compliance with the requirements for EMC IEC-61850-3;
• average time between failures of at least 150,000 hours;
• service life not less than 15 years;
• support for operating systems Windows, QNX, Linux.

The following configuration was created for the filtering device: Intel Core i3-5010U 2.1Ghz processor, 2 cores, 8GB RAM, 4 Intel I210-T1 GbE ports.

4. Experimental study

Test studies of HTTP filters are necessary in the form of bench tests to determine the performance and ultimate characteristics, as well as to conduct a comparative analysis of the filtering methods used. They are carried out both according to the standard scheme, and according to the scheme with the separation of functions between an industrial computer and a programmable switch, which was used as MicroTik RB 260GS. The experimental approach used to study filtering devices was developed and described in [11]. The test bench was created on the basis of a dedicated local area network in which computers - emulators of Web clients and Web servers are combined, as well as a filtering device placed in the gap between them (Figure 5).

![Figure 5](image)

Figure 5. Testbed configuration and interaction scheme of its software modules for testing the computer model of the HTTP filter.

At the stand, an imitation of the operation of the production subsystem was performed. Multiple requests by clients to built-in web servers passing through the filtering device occurred. For this aim a special software module (C) is installed on the computer intended for emulating Web clients, which send requests to another computer with a software emulator of the Web server (S), which creates and sends back the answers to received requests. In accordance with the filtering rules, the HTTP filter (F) regulates access to server resources (Figure 5). The measurement software module (M) is located on the Web client emulator. With it, the parameters of test traffic and a number of characteristics of the filtering device are determined.

During testing, the intensity of the input stream (the number of requests per second) and the size of the response from the web server (1Kb and 100Kb) were varied. At the same time, waiting time of the response from the server (in seconds) and the filter capacity (number of requests per second or megabits per second) were measured.

The task of the experiments included imitation of the following situations:
a) there is no filter in the system,
b) the filter operates in the standard mode described in [7,8] (the configuration is shown in Fig. 2),
c) the filter operates in enhanced (post-analysis) mode described in [9] in conjunction with the MikroTik programmable switch (configuration is shown in Fig. 3).

The results of the tests, made in the form of graphs of the dependence of the waiting time of the response of the web server in seconds on the intensity of the sent requests in Mbps are presented below. Figure 6a shows the graphs of experiments in which the size of the response from the web server is 1Kbyte, and in the Figure 6b it is 100Kbyte.

In both graphs, the lower curve represents the simulated situation A), the upper one - situation B), and the curve between them, situation C).

![Graphs of the dependence of the waiting time of the response of the web server in seconds on the intensity of the web traffic in Mbps: a - size of the response is 1Kbyte; b - size of the response is 100Kbyte.](image)

Figure 6. Graphs of the dependence of the waiting time of the response of the web server in seconds on the intensity of the web traffic in Mbps: a - size of the response is 1Kbyte; b - size of the response is 100Kbyte.

According to the results of the tests, it turned out that when exchanging short messages, the download of the communication channel between the client and the web server does not exceed 454 Mbps in the absence of a filtering device on the line. This is due to the fact that during a communication session, the exchange goes through short messages, between which pauses occur. If there is a filtering device on the line, then the traffic reaches 240 Mbps with the standard filter operation mode and 338 Mbps in the post-analysis mode when installed in conjunction with the MicroTik programmable switch. This amounts to 52.9% and 74.4% of the maximum value.

When exchanging long messages, the gigabit channel is fully loaded. The filtering device allows traffic up to 849 Mbps in standard mode of operation and up to 931 Mbps in post-analysis mode paired with MicroTik programmable switch.

The experiments showed that, depending on the size of the response from the web server with the standard algorithm, the filtering device reduces the throughput of the communication channel by 15% - 47%. When using the improved algorithm - by a value from 7% to 25%. Also, when using the improved algorithm and its hardware support, the response time from the Web server is reduced to 2.2 times, and throughput is increased to 1.4 times.

5. Conclusion

For the regulation of access to devices of the Industrial Internet of Things and their individual capabilities using the HTTP protocol, one of the possible options is to use a filtering device on an industrial hardware platform. It can be used in conditions of increased requirements for operating conditions as part of industrial automated control systems built using IIoT technology as a mean of increasing information security. The filter can be applied both with a standard and with an improved algorithm based on the application of the method of post-analysis of requests with its hardware support.
support. In the study, the use of an improved algorithm for the Gridex-II platform, together with its hardware support, reduced the waiting time for a response from the web server to 2.2 times and increased the filter throughput to 40%.

Acknowledgments
The reported study was funded by the Ministry of Science and Higher Education of the Russian Federation. Projects # АААА-А17-11706061006-6 and #АААА-А17-117062110016-4.

References
[1] Hermann M, Pentek T and Otto B 2015 A literature review In Design principles for Industrie 4.0 scenarios(Technische Universität Dortmund, Dortmund). Retrieved from: https://www.thiagobranquinho.com/wp-content/uploads/2016/11/Design-Principles-for-Industrie-4-0-Scenarios.pdf.
[2] Wallis E 2020 How the internet of things speeds up industry 4.0 Progress Forbes Retrieved from: https://www.forbes.com/sites/sap/2020/03/04/how-the-internet-of-things-speeds-up-industry-40-progress/#4f01ee8b5998.
[3] Sisinni E, Saifullah A, Song Han, Jennehag U, and Gidlund M 2018 Industrial Internet of Things: challenges,opportunities, and directionsIEEE Transactions On Industrial Informatics.
[4] Shaw K 2019 What is edge computing and why it matters Networkworld Retrieved from: https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html
[5] Greenfield D 2012 Industrial networking desires revealedAutomationWorld Retrieved from: https://www.automationworld.com/products/networks/article/13308055/industrial-networking-desires-revealed
[6] Real Time Logic 2020 Device management via iot or embedded web server? Whitepaper Retrieved from: https://realtimelogic.com/articles/Device-Management-via-IoT-or-Embedded-Web-Server
[7] Balasubrahmaniyan J, Daftary K, Yarlagadda V R and Kumar K 2006 System and method for url filtering in a firewallPatentUS 20060064469A1 Int. Cl.G06F 15/16 (2006.01), Pub. Date: Mar. 23, 2006.
[8] Bloch E, Mohan S, Pagaku R R, et al. 2010 Apparatus for monitoring network trafficPatent US 7849502 B1, Int Cl G06F 15/16 (2006.01), G06F 11/00 (2006.01), Pub. Date: Dec. 7, 2010.
[9] Budnikov K I and Kuruchkin A V 2019 Software modelling of network traffic filtering process in information system regulating the access to Internet content via HTTPJournal of Physics: Conference Series1353 012129. DOI: 10.1088/1742-6596/1353/1/012129
[10] Tornado Modular Systems Limited Liability Company 2018 Industrial computer GRIDEX II. ABNS. 431295.007.RP Application Guide(Novosibirsk). Retrieved from: URL: https://ipc-gridex.ru/upload/iblock/75d/75dce82525c0bce8ee5a55a9a33d95efe.pdf
[11] Budnikov K I, Kuruchkin A V, Lubkov A A and Yakovlev A V 2018 Experimental study of symmetric computer model of http-filterIn Proc. of the 2018 3rd Russian-Pacific Conf. on Computer Technology and Applications (RPC)( Vladivostok). DOI: 10.1109/RPC.2018.8482147, URL: https://ieeexplore.ieee.org/document/8482147