Adaptive Industrial IoT Security Threats Intelligent Perception "Robots"

Allam MAALLA\textsuperscript{1}, Yong GUO\textsuperscript{2} and Shu-qing LIN\textsuperscript{1}

\textsuperscript{1}Research Institute of Open Data Commercial Application, School of Information Technology and Engineering, Guangzhou College of Commerce, Guangzhou, China
\textsuperscript{2}ZTE Corporation Company, ShenZhen, China

\textbf{Keywords:} Internet of things, A comparative analysis of security enterprises, Industrial IoT.

\textbf{Abstract.} This paper concept to study the security of the automatic discovery method of the threat under the industrial space. By building an adaptive cyberspace security threat to intelligent perception of "robots", the use of its "complex eye" sensor adaptive perception, continuous perception of complex and changeable network space behavior and state changes; Using its tentacles data, automatically connect to a variety of threats from different sources of information; use of its powerful central control intelligence analysis capabilities, self-learning every day, like the alpha dog of self-evolution, accumulating abnormal behavior and threats in cyberspace knowledge base; Using its unique language man-machine cooperation and collaboration security experts, update cyberspace threats and abnormal behavior characteristic of knowledge; finally able to automatically identify threats, and timely warning.

\textbf{Introduction}

The Ministry of Industry and Information Technology issued a "industrial control system information security protection guide" to guide industrial enterprises to carry out industrial safety protection work. "Guide" to the "security is the premise of development, development is the security " to the current industrial control system in China facing the security issues as the starting point, pay attention to the enforceability of the protection requirements, from the management and technical aspects of industrial enterprises to clear industrial safety Protection requirements.

Traditional security products in the design concept, product architecture and functional design and processing capacity, is based on the traditional security concept to determine the security protection scenarios and the appropriate network size and data volume, only suitable for solving the traditional enterprise network space of a single , The security control of the scene, not suitable for the Internet of things security control scene; because the application of complex things network, the network size continues to expand, the amount of data increased dramatically, network attack behavior changes are also increasing.

\textbf{Current situation, Level and Development Trend (Internet of Things)}:

China 's major Internet of things security enterprises Mainly divided into two categories: one is based on the construction of things was to provide intelligence gateway, which represents the business is Weston Information Industry Company Limited; one is for GAINS actual construction was to provide comprehensive solutions for the Internet of Things. Foreign typical Internet security companies are: The USA Verayo company, mainly to provide RFID security technology and products\cite{1}. Netherlands Intrinsic-ID company, is committed to improving the Internet of things terminal device security; US wind River company, mainly to provide terminal equipment open software environment and the overall network security solutions \cite{2}.

\textbf{Constructing Intelligent Analysis on iHOS Based on Big Data}

This paper from the perspective of adaptive safety control concept to study the industrial space under the security of the threat of automatic discovery method. Through the construction of an adaptive cyberspace security threat, the intelligent perception of "robot", the use of its "complex
eye" sensor adaptive perception, continuous perception of complex and changeable network space behavior and state changes; use of its data antenna, automatically connected from different Channel of the various threat information; the use of its control center strong intelligent analysis capabilities, self-learning every day[3,4], like the Alpha dog as self-evolution, and constantly accumulate network space behavior anomalies and threat knowledge base; use of its unique man-machine coordination language and security experts Synergistically, updating cyberspace behavior anomalies and threatening knowledge characteristics; and finally automatically identifying threats and prompting alerts.

Figure 1. Constructing Intelligent Analysis on iHOS Based on big data.

A Comparative Analysis of Security Enterprises:

Enterprises in the perception layer, application layer security research with foreign countries have a big gap. In terms of perception layer, due to the weak foundation of material, technology and other sensor technology innovation ability is insufficient, and therefore less safe conduct research in RFID and other related businesses perception layer. The key technology in the network layer is the basic synchronization with foreign countries, so the security gateway vendor related research and development results are applied to things safe. In the application layer, China is both middleware or software are more use of IBM, Sun and other foreign company products, embedded in the equipment development environment is also dependent on Wind River's software development platform[5] . In addition, cloud computing and cloud computing security and other Internet applications layer, the domestic technology research and development is also lagging behind.

Enterprises focus on technological innovation and technology optimization, China's enterprises in this area is weak. Foreign security companies have started all safety-related research in the concept of things just made, focus on technological innovation and advance research. Moreover, Wind River and other foreign security companies by the optimization of existing cutting-edge IT security control methods to adapt things information security needs. In the domestic, due to the development of things in the initial stage, although many concerned about the Internet of things security business and experts, but due to there is no strong market demand, so specializing in Internet of things security product development and Internet security solutions for fewer enterprises.

To promote the application of their own products; Wind River and Hewlett-Packard companies, the joint launch of the corresponding products, better adapted to the evolving network infrastructure. Domestic enterprises in cooperation with the industry chain downstream side also weak.
Enterprises in terms of easier access to venture capital support, domestic enterprises more dependent on government financial support for the project, limiting its direction of innovation and applications. In the enterprise development funds, foreign companies are relatively easy to obtain venture capital, Verayo company itself is set up by the venture capital company, and Intrinsic-ID company, to promote the company’s core technology development and application through financing to obtain 5 million euros support, Enterprises can according to their own business direction and focus on free control of venture capital or financing funds. In the domestic, enterprises rely more on government project funding support, Guardian pass in the domestic information security industry has a place, but its security aspects of things mainly rely on government project funds, and other sources of funding less, which determines its innovative direction or new Technology applications are dominated by government.

Figure 2. Adaptive security intelligent Business Architecture.

Figure 2 shows business-oriented man-machine collaboration language Solve the "robot" and security business expert’s smooth communication and coordination issues.

Internet of Things Technical Feasibility Analysis

Internet of things mature and steady development, there are already many companies into which the relevant technology has become more mature. This includes professional companies that make industrial data connections, industrial large data analysis companies, and AI intelligent robots. Many enterprises have achieved the relevant technology; technical feasibility can be fully proved.

Necessity Analysis

With the development of science and technology, the automation degree of modern industrial production is more and more high, but the system resources of industrial control system is limited, the system efficiency and real-time related network characteristics are considered at the beginning of the design of network protocol, and there is not enough attention to the safety of industrial networking, and the industrial IoT protocol itself is immature, As well as the fast-changing virus and network attack means, the security problem has become one of the main bottlenecks restricting the development of industrial IoT. Therefore, how to effectively ensure the safety of industrial networking is imminent.
Adaptive Security Intelligent Business Architecture

With the development of science and technology, the degree of automation of modern industrial production is getting higher and higher, but the system resources of industrial control system are limited. At the beginning of the design network protocol, only the system efficiency and real-time network characteristics are considered, Security issues have become a major bottleneck restricting the development of industrial networking; in addition, the industrial networking security problem is a country. The security of the industrial networking problem is a country. Therefore, how to secure the security of industrial products by state-owned security products is imminent, and we hope that the research results of this project will be shared.

Industrial networking applications are complex, a wide range of network elements, different industrial protocols and communication protocols intertwined, a variety of network behavior intertwined, frequent data exchange, making the industrial networking data presented four characteristics: large amount of data, data quality sparse, Data types and formats are complex, data relationships and real-time correlation with the application scene at the same time, network abnormal behavior and security attacks and normal network communication behavior intertwined, which makes industrial networking security threats to identify more difficult.

Summary

Using Industrial IoT behavior data adaptive sensing ability To solve the problem of data collection capacity of IIoT, And to solve the problem of how to effectively identify the network behavior (normal, abnormal, attack) in the environment of industrial networking, in order to deal with the diversity of communication protocols and applications. Industrial IoT behavior real-time correlation computing capacity of the adaptive expansion Solving the Real-time Correlation Computing Capability of Network Behavior Data and Related Scene Characteristics of Industrial Internet.
Acknowledgement

This research was financially supported by Characteristic Key Subject of E-commerce Construction Project of Guangzhou College of Commerce Foundation, project No. TSZDKX201601. And National Natural Science Research Project "Project Title: Construction and Application of E-commerce Big Data Analysis Platform (Third Party), project No. (17BQNS01002).

References


