Journal of Theoretical and Applied Information Technology
15th December 2012. Vol. 46 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURITY ANALYSIS FOR INTERNET OF SHIPS

[1, 2, 3]QI JING, [1]LI CHENG

[1]School of Software and Microelectronics, Peking University, Beijing, P.R.China

[2]Key Laboratory of High Confidence Software Technologies (Peking University), Ministry of Education, P.R.China

[3]Key Laboratory of Network and Software Security Assurance (Peking University), Ministry of Education, P.R.China

ABSTRACT

With the development of water shipping technology, research and construction of the waterway information technology has received much more attention. However, smart shipping system still faces many problems, such as the shipping management is sufficiently sophisticated the services are not comprehensive, our travel is not humanistic, and the security is not enough. As an emerging interdisciplinary research focus, the internet of ships is proposed to solve these problems. Based on the analysis of the construction of the shipping information management and service, as well as the main problems existed, this paper focuses on the basic architecture and features of the internet of ship, explore the security problem existed in the internet of ship, and list issues need to be addressed in terms of security of internet of ship clearly.

Keywords: *Internet of Ship, AIS, Intelligent Shipping System*

1. INTRODUCTION

With the development of shipping technology, more and more ships begin to engage in the water transport. However, we still lack effective real-time water information management system, and also, we are lack of effective means of information exchange between the ships, ship-to-shore, and ship internal, and there are serious of security transport problems lying in the waterway transportation. Therefore, how to manage the water transportation smartly and effectively has become a more and more urgent problem. Internet of ship is proposed to solve this problem.

1.1 Internet of Ships

Internet of ships, are to connect ships and base station with network. It is a kind of network based on the technology of internet of thing, armed at realizing more refined shipping management, more comprehensive industry service, as well as more humanistic travel experience.

Internet of ships, introduces the concept and technology of the Internet of Things [2] into the field of inland navigation, and it is a new direction, with a certain degree of creativity and exploratory. In the context of the vigorous development of the Internet of Things industry, the field of river information services gradually highlights that the shipping management is sufficiently sophisticated, the industry service is not comprehensive, our daily travel is not humanistic, and the security is not enough and various other shortcomings. In addition, the traditional land-based road transport and logistics system endures the higher load pressure and management costs, which presents emerging demand for the construction of internet of ship. In a word, the successful construction of the internet of ship can enhance the intelligence, security, efficiency and environmental protection of the water transport, which can inject new blood into the traditional logistics transportation.

1.2 Status

The EU launched a pan-European river information services system [3] (RIS) demonstration project in 2006. Through the construction and perfection of ship tracking and tracing system, electronic message system, inland electronic chart and display systems and other shipping infrastructure, European countries have established their own integrated information service system, making up the pan-European river information services system covering the Rhine and the Danube basin [4], which can provide traffic management, traffic information, logistics information, emergency rescue and other eight information service function, realizes the pan-European inland river shipping transportation efficiency, safety, and environmentally.

In China, on May 7, 2004, the first phase of construction of the Yangtse River delta ship automatic identification system (AIS) station network system run successfully. It is consist of four AIS base stations in Huaniao hill, Dagan hill, Hengsha, Wusong and an AIS center in the Shanghai beacon, the network of this system cover the whole of the Yangtze River estuary. At the same time, the Pearl River Estuary AIS station network system also run successfully and smoothly, the and the system cover the entire Pearl River estuary waters, including Guangzhou, Shenzhen, Hong Kong, Macao and other ports in Pearl River delta.

2. ARCHITECTURE

2.1 The Main Architecture of The Internet of Ships

We know that the Internet of Things has three characteristics, which are the overall perception, reliable transmission and intelligent processing. As the application of Internet of Things technology in the water shipping, Internet of Ships should also satisfy these three characteristics. Therefore, we can divide the internet of things into three layers that are the perception layer, the network layer and the application layer. Perception layer is mainly responsible for the perception of the ship data networking systems, the network layer is responsible for the communication and exchange of information between the various of nodes in internet of ships, the application layer to provide a variety of functions, including navigation, early warning, monitoring, information services, as shown in Figure 1.

2.2 Perception Layer

The perception layer is mainly used to perceive various data in the internet of ship system. In the system, we need to use a variety of means to comprehensively collect the information of goods, vessels, aids to navigation, waterways, ship locks, bridges and other information. For example, we use the marine RFID tags to carry out ships identification, goods identification, and get the information of the type of goods, quantity and destination. We can use radar [5], AIS, GPS and Compass technology to get the position of ships and beacons, the heading, speed and other information. At the same time, the use of fieldbus can help us access the running state of ship equipment, the ships around, the information of water depth. Besides, by using temperature, humidity, wind speed, wind direction, rainfall, atmospheric pressure, visibility, currents, water depth, oil spills and other various sensors, we can get the meteorological environment, waterway information. In addition, by using laser, ultrasonic sensors, we can get the ship's positioning the ship lock, bridge clearance and the navigable width.

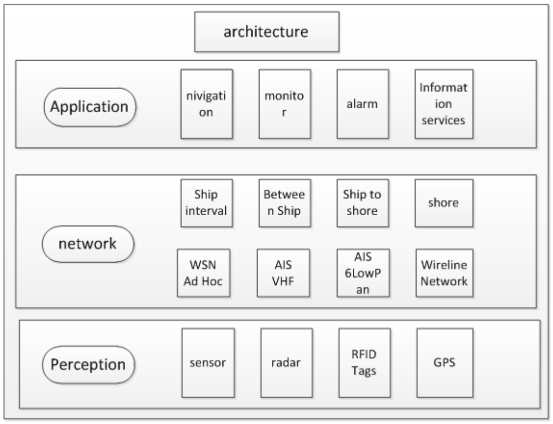

Figure 1: The Architecture Of The Internet Of Ships

2.3 Network Layer

The network layer is mainly responsible for the communication and exchange of information between the nodes in Internet of Ships. In the system, the exchange of information between nodes can be mainly divided into four parts: the internal ship information exchange, information exchange between ships, information exchange between ship and shore, and exchange between shore stations. Each part of system use different protocols and technology, and at the same time, by constructing heterogeneous networks between different parts, we can carry out the interaction of information. In the interior of the vessel, we can set up a wireless self-organizing network (Ad Hoc) [6] and wireless sensor network [7] (WSN) to convey information; between the ship, we can use the AIS, VHF, satellite networks to exchange information; in the ship and shore, we can use AIS, VHF, 6LowPan technology and so on; as for the shore between systems, we can use the traditional wired network for information communication.

As can be seen, in the internet of ships, there are many kinds of network. When so much of network exchange information by the convergence of heterogeneous networks, there could be various security issues, And we will discuss the problem in the following security analysis in section 3.

2.4 Application Layer

The application layer provides a variety of functions, including navigation, early warning, monitoring, and information services. The application layer is constructed above the network layer, through the integration and analysis of the data transfer over the perceptual layer transfer, the application layer can provide various service functions for the staff on ship and shore station. For example, the navigation services, which can provide line navigation function for the ship, early warning, which can for provide timely warning information for ships on the water, monitoring, which can monitor the water ship running line, speed, and information services, which includes the ship location information services, logistics information service, enterprise information services.

3. SECURITY IN INTERNET OF SHIP

From the above framework, we can see that, there are many kinds of security problems lying in the terms of internet of things. In the system, the information exchange can be divided into four main parts: inside the ship, between the ship, between ship and shore stations, and between systems on the shore station. Each part of the internal use different protocols and technology, and at the same time, we usually carry out the interaction of information by constructing heterogeneous networks between different parts. In addition, the internet of things itself also uses some special system, such as AIS. All of these are likely to come under attack, leading to the leaks or misinformation of information, and impact the whole internet of things system. Therefore, we can discuss the networking security in the internet of ships from the following three aspects.

3.1 Security Analysis in Perception Layer

From the above framework analysis, we know that we need use a variety of equipment and technology to collect data, such as many kinds of sensors, radar, RFID tags, GPS, and Nova technology. As the security issues in the internet of things, these are susceptible to the attacker's interference, shield and the signal interception. At the same time, after the acquisition of data, we need to use a variety of means of communication to transmit these information, such as RFID, MF/HF, GPS, 3G, AIS, WSN, Wimax, VHF, GPRS, microwave, if these techniques used in the protocol get attacked, it is likely to cause leaks or misinformation of information, which may impact the whole network of the internet of ships.

Through the above analysis, we know that as the sensor nodes in internet of things, the sensor nodes in internet of ships are also deployed in some unmanned monitoring environment, with weak ability, limited resource and other features. In this case, the sensor node is easy to suffer physical damage from the attacker. The attacker can easily access to the sensor device, and by the use of some illegal means, they can capture sensor nodes, then destroy or replace some of these nodes. As a result, we cannot collect the right data of the internet of ships system, let alone the follow-up analysis and processing work. At the same time, because of the limited capacity and resources of the perception nodes, they cannot carry out high strength encryption operation. Therefore, the encryption algorithm commonly used is no longer in force in this occasion. Furthermore, these nodes cannot communicate in long distance safely. These lead that the sensor signals are easily interference, shield or intercepted by the attacker. Once thus happens, the network layer will no longer accept the right data collected by the sensors, as a result, the following analysis and processing work will get affected obviously.

Let us take radio frequency identification (RFID) as an example. RFID is also known as electronic label, is a kind of communication technology. Through the use of radio signal recognition of specific goals, RFID can help us read and write data, without the need for the mechanical or optical contact between the recognition system and specific target. in RFID technology, we mainly use 2 frequency signal, a low frequency signal with short transmission distance, and the main frequency is 125kHz, 225kHz and 13.65 MHz; the other is a high frequency signal and the microwave with long transmission distance, and the main frequency is 433MHz, 915MHz, 2.45GHz and 5.8GHz. Now each band of the electromagnetic wave signals is in use, so the adjacent channel interference between the neighboring bands is great. The immediate impact brought by interference is the data error in the reader and tag communication.

When the label receives the commands and data from the read / write devices, if they get attacked by the attackers, then it will lead to the following wrong results. The label responses to readers' command incorrectly; the label work state is confused; the label get write error or enter a state of dormancy.

On the other hand, when the read/write device get data information from the label, if they get attacked by the attackers, thus may lead to the following errors: the read/write device cannot recognize the normal working label; the devices identify an label as another label, cause recognition errors; the signal are intercepted by attackers, then the attackers send information to reader by posing as RFID label; the reader launch specific electromagnetic wave which may damage the data inside the label. Besides, due to the cost constraints, a lot of labels are not possible to use a strong programming and encryption mechanism, so the illegal user can use legitimate reader or construct a reader to communicate with labels. Thus the label internal data are easily being stolen, and for those label which can read and write data will also face the risk of data being modified. In addition, between the reader and Host (or application), the attackers can also modify the configuration files directly or indirectly, through which they can eavesdrop and interference the exchanging data.

3.2 Security Analysis in Network Layer

In the foregoing analysis of the architecture analysis, we know that large-scale internet of ships mainly includes four aspects: network within the ship, network between the ships, network between ship and shore, and network between the shore system. In internet of ships, it contains many kinds of networks, such as AIS, VHF, cellular mobile communication network, satellite network, GPRS, WLAN, mobile ad hoc network (MANET), Wi-Fi, wireless sensor network (WSN) etc.. At the same time, each aspect of network may consist of several ways of formation, finally forms a heterogeneous network environment. Because of the openness of the wireless channel, the wireless link is vulnerable to get security attacks, and thus is behaved more apparently in heterogeneous wireless network environment. Besides, the security mechanism in different types of wireless networks is different and intensity, and the safety strength is not unified, so network with weak security protection in heterogeneous network is easily become the breach of heterogeneous network attack, which poses a serious threat to the security of the whole heterogeneous network. Heterogeneous network interconnection lacks enough security protection for the equipment and the devices, therefore, the equipment and devices are susceptible to get link attack, including tapping, flow analysis, illegal access and DoS attack. Once they are attacked and destroyed, it often leads to other network getting affected, resulting in the whole internet of ships system unsafe. Here, we carry out the safety analysis to several key technology and network in internet of ships. They are Ad Hoc, WSN, and 6LoWPAN.

3.2.1 Ad Hoc network security analysis

In the interior of the vessel, we can set up the Ad Hoc network for information exchange. Ad Hoc network is a centerless self-organized wireless network, it is not based on any existing fixed infrastructure and can set up temporary network whenever and wherever. It is a peer to peer network for special purpose, by using the wireless communication technology, the nodes in the network as its neighbors (in its direct communication within the node) router, via the forwarding between nodes to achieve communication between nodes. Because of its dynamic topology and wireless communication, the Ad Hoc network is vulnerable to suffer security threats.

In the Ad Hoc network, there is no base station or central node, all nodes are mobile, and the network topology often changes dynamically. At the same time, nodes in Ad Hoc network connect through wireless channel, there is no dedicated router, so the node itself should act as a router. In addition, there is no name service, directory service or other network functions. As a result, Ad Hoc network is more vulnerable to all kinds of security threats than the fixed network, such as tapping, forged identity, playback, tamper message and the denial of service and so on.

Ad hoc network is subjected to security threats in the following aspects. In the transmission channel aspect, the Ad Hoc networks using wireless signal as the transmission medium, the information transmits over the air. Not likely the wired network, we have to cut the communication cable and lap to eavesdrop, in Ad Hoc network, anyone can receive message, so it is easily bugged by attackers, and the wireless channel is vulnerable to jamming and implanting false message by attackers. In the node mobility aspect, because the node is independently movable, unlike in the fixed network, nodes can be placed in the security room, in the Ad Hoc network, the node’s security is very fragile. The mobile node may fall into attackers’ hands, the key of nodes, message information may be cracked by attackers, then the node may join the network again without being penetrated. As a result, the attackers can use these nodes to obtain secret information and destroy the network's normal function. Therefore, Ad Hoc network not only has to guard against external invasion, but also has to deal with the internal nodes of the attack. In dynamic topology aspect, Ad Hoc network nodes’ location is not fixed, and can be moved at any time, thus causing the network topology changes. A correct routing may be unreachable due to the destination node moving out of the range and, or suspended due to the intermediate nodes removing and breaking off in the routing path. Therefore, it is difficult to difference the reason of a wrong route, maybe it is caused by the nodes’ moving or the false routing information. Because of the node’s mobility, when the attack is identified somewhere, it can move to a new location, change the logo, and join the network again. In addition, due to dynamic topology, the network has no boundary, the firewall also cannot be used properly. In the security mechanism aspect, in the traditional public key crypto system, we can use digital signature, encryption, message authentication code and other technology to realize the information confidentiality, integrity, non-repudiation and other security services. However it needs a trusted authentication center to provide the key management service. But in Ad Hoc network, the network will not allow the existence of a single authentication center, otherwise if the individual certification center collapses, it will cause that the entire network cannot obtain certification, and the attacker can get the private key, use the private key issue false certificates, which causes the network completely losing safety. By the backup center of attestation, we can improve the survivability, but it also increases the target, if any certification center is breached, the network will lose safety. So, in the Ad Hoc network, we cannot use the traditional confidential mechanism. As a result, the attacker is easy to decipher the message in the network. In the routing protocol aspect, in Ad Hoc network, routing algorithm assumes that all nodes in the network are mutual cooperated to complete the network transmission of information. If some nodes in the network stop forwarding data to save resources, it will affect the performance of the entire network. More serious, if the attackers broadcast false routing information, or deliberately spread a lot of useless data packets, thus may cause the entire network crashing.

From the above analysis, we can see that the Ad Hoc network faces many kinds of security problems. As a result, when we use Ad Hoc network in the internet of ships, we also have to face these security problems. And if we cannot deal with these security problems properly, once the Ad Hoc network suffers the attack from attackers, the consequences often blows up with the network communication between the internet of ships, leading to more serious problems.

3.2.2 WSN security analysis

In the interior of the vessel, and between ship and shore system, we can set up a WSN for information exchange. Wireless sensor network (WSN) consists of large number of sensor nodes deployed in the monitor region. These nodes form a multi-hop self-organizing network system through wireless communication. The WSN can help us collaborate to perception, get and process the object information been sensed in the network coverage area and send to the observer.

However, in WSN, a single node has constraint resource, including processor resource, memory resources and power. Therefore, the node has limited processing power, can't carry out complex calculations. At the same time, the node is unattended, so it’s fragile and vulnerable to suffer physical attack. Besides, nodes may be mobile, the transmission medium is not reliable, and the network has no fixed infrastructure, these resulted in WSN vulnerable attacked by attackers.

WSN is subjected to security threats in the following aspect. In Physical node aspect, the node may get attacked. Physical node attacks aim at carry out destructive behaviors to node itself physically, including the distortion, damage, replacement or adding of physical nodes. As a result, the attacker can steal the node key information or carry out other attack throughout the change or replacement of these physical nodes, such as adding nodes to blocking network communication. In the transmission channel aspect, due to the shared medium feature of wireless communication, the attacker can make the legal communication unused by occupying the channel for a long time. The attacker also can monitor link flow, steal key data or obtain important information through the analysis of packet head field to carry out the follow-up attack. In packet information aspect, the attacker can make threat to WSN by forging wrong packet information. They attack can also tamper packet to attack WSN. The attacker can use the malicious nodes to change the legal route package head field, which can interfere the normal routing process, or destroy data load to manufacture error data. Attackers may also discard packet. they can break out the legal process of packet forward by discarding packets that should be forwarded to other nodes. The attacker can reduce the priority of packets from other nodes or refuse the forwarding of these packets, thus may bring bad effect to the network availability and quality of service. The attacker can also forward packets maliciously. By introducing errors in forwarding behavior, they can reduce the network efficiency, make the communication between nodes out of use. In the collaborative aspects, attackers can manipulate the global routing information through the cooperation of one or more nodes, thus can disrupt the normal route activities, and provide convenience for follow-up attacks.

3.2.3 6LoWPAN security analysis

We can use 6LoWPAN in communication between ship and shore.6LoWPAN is carried out in the IEEE 802.15.4 PHY/MAC layer, by the construction of IPv6 protocol stack, it introduces the IP protocol to the wireless communication network. It has low power consumption, low throughput features, and it is consist of the equipment which follows the IEEE 802.15.4-2003 standard, these devices have a short distance, low bit rate, low power consumption and low cost features. The IPv6 is introduced to the wireless sensor network, brings the advantages of IP network, but at the same time, it also brings in the current IP network security problems.

The security problems that 6LoWPAN faces can be divided into two major parts, they are external attack and attack inside. External attack means that the attacker outside the 6LowPan network attack the network through eavesdropping signal tampering with the network data packet, and send attack packets to the network. The attack inside refers to that the attacker personates to a part of an 6LoWPAN network based on the analysis of the data collected from the network, then the attack can obtain certification, authentication, confidentiality encryption algorithm etc..

Therefore, when we use 6LoWPAN in the internet of ships, we possibly suffer attack because of the 6LoWPAN security problems, causing information leakage and the networking system working incorrectly. For example, the 6LoWPAN network may be subject to denial of service (Dos) attack. IEEE 802.15.4 uses CSMA/CA (Carrier Sense Multiple Access / collision avoidance) mechanism to solve the channel assignment problem. In this mechanism, if a conflict is detected, we have to repeat the packet, so the attacker can send the data packet purposely to cause conflict. As a result, the nodes have to constantly retransmit data and stop work finally due to the using up of limited energy. Thus will make the 6LoWPAN network paralyzed. At the same time, because 6LoWPAN is a wireless network, so the information transmission is vulnerable to get attacked, including tapping, tamper, implantation, interrupt and flow analysis. In addition, we know that the 6LoWPAN network is generally arranged in an unmanned open environment, and the node is cheap, simple designed, so the attacker can completely replicate a new acceptable control node according to the existing node, and add it to the network, which can collect the needed information. Once the 6LoWPAN is subjected to the attacks above, it may lead to the 6LoWPAN network paralyzed, information leakage, or error information spreading. These effects will further amplify throughout the internet of ships system, thus causing the entire systems security problem.

3.3 Special System Security Analysis

In the internet of ships, the AIS (Automatic identification System) has been widely used. IMO(International Maritime Organization) provisions that all international navigation ships with the gross tonnage over 300 tons, and all Non-international navigation ships with the gross tonnage over 500 tons, and all passenger ships, are required to be equipped with AIS.

AIS [10] is a technology based on self-organizing time division multiple access [11] (SOTDMA) wireless communication system in marine, it exists the defects. When the ships and the shore stations communicate using AIS, if the SOTDMA emission time slot is got by the attacker, the attacker may launch interference or falsification of information with higher power, then the recipient may can't receive information or receives error information, resulting in a serious traffic accident or privacy leakage incident, all of this will break out the normal work of the internet of ships system.

4. CONCLUSION

The development of internet of ship, will significantly enhance the intelligent level of the waterway transportation, and provide more humanistic and refined services for shipping management, industry services, people's daily travel and so on. Based on the analysis of the construction of the shipping information management and service, as well as the main problems existed, this paper explains the basic architecture of the internet of ship, as well as the features of individual part. This paper also explores the security problem existed in the internet of ship, and lists the issues need to be addressed in terms of security of internet of ship clearly.

ACKNOWLEDGEMENTS

Li Cheng is the corresponding author of this paper.

REFRENCES:

[1] N. Booij, R. C. Ris, L. H. Holthuijsen, "A third-generation wave model for coastal regions: 1. Model description and validation", *Journal of geophysical research*, Vol. 104, No. C4, 1999, pp. 7649-7666.

[2] Yinghui Huang, "Descriptive models for Internet of Things", *Proceedings of 2010 Intelligent Control and Information Processing*, Augest 13-15, 2010, pp. 483-486.

[3] J. Vallant, B. Hofmann-Wellenhof, “River Information Services”, *e & i Elektrotechnik und Informationstechnik*, Vol. 125, No. 6, 1999, pp. 238-243.

[4] R. Pfliegl Dr., “Neue Wege des Verkehrsmanagements auf Binnenwasserstraßen — River Information Services auf der Donau”, *e&i Elektrotechnik und Informationstechnik* , Vol. 120, No. 1, 2003, pp. 42-49.

[5] Challamel, R., “A European hybrid high performance Satellite-AIS system”, *Prodeedings of Advanced Satellite Multimedia Systems Conference (ASMS)*, September 5-7, 2012, pp. 246-252..

[6] Fei Hu, Neeraj K. Sharma, “Security considerations in ad hoc sensor networks”, *Ad Hoc Networks*, Vol. 3, No. 1, 2005, pp. 69-89.

[7] Kun Chang, Qingwei Liu, Mandan Liu, Hailong Xiong, “The Mechanism of Abnormal Detection and Distributed Localization of Nodes Based on Trust Management in WSN”, *Proceedings of 2012 Asia Simulation Conference*, October 27-30, 2012, pp. 422-430.

[8] Qi Jing, Jianbin Hu, Zhi Guan, Zhong Chen, “TEAMA: Trust Evaluation Based Authorization Model for Ad Hoc Networks”, *Proceedings of the 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control*, October 21-23, 2011, pp. 470-474.

[9] Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen, “Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks”, *Journal of Network and Computer Applications*, Vol. 35, No. 3, 2012, pp. 1001-1012.