Concealment of sensor network node interaction

E A Kushko and N Y Parotkin
Institute of Informatics and Telecommunications, Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russian Federation
E-mail: evgeny.kushko@gmail.com

Abstract. The aim of this study is to increase the security of sensor network hosts by means of node interaction concealment. This paper outlines existing methods and approaches to information security of sensor network and internet of things systems. The authors developed a new secure data communication method based on dynamic network topology. This method allows to conceal sensor network data communication from an intruder breached an outer security perimeter. The new method secures data transfer and differs from the existing switching approaches that conceal sensor network hosts.

1. Introduction
The Industrial Internet of Things (IIoT) is a multi-level system that consists of sensors, various industrial nodes and unit controllers, means of collecting, transmitting and processing data, as well as analytical tools, data visualization tools and other components. This system is designed for offline data collection and real time data communication and enables remote monitoring and management of industrial facilities with no (or minimal) human involvement. Industry 4.0 assumes widespread introduction of industrial Internet of Things in various economic sectors since it aims to create automated cyber-physical systems collecting, processing, visualizing and systematizing data, and thus implementing and controlling various industrial processes [1].

The lower layer of the industrial Internet of things is a wired or wireless sensor network. The sensor network is a dynamic, distributed, self-organizing network of sensors and execution units, which is designed to accomplish automation, diagnostics, telemetry and machine-to-machine interaction tasks. The following requirements are considered when building a sensor network: ease of deployment and operation, no need for frequent maintenance, high fault tolerance and reliability, as well as low performance and bandwidth requirements [2]. The industrial Internet of Things has a positive economic impact in various industries, so the number of such systems is increasing. However, with the spread of the industrial Internet of Things, the number of attacks on these systems is also increasing.

2. Sensor network security measures
Usually, one can protect traditional local networks with layered defense, network segmentation, monitoring and managing network traffic, concealing the architecture and configuration of the information system, encrypting transmitted data, providing trusted channels and routes, ensuring the authenticity of connections and building a security perimeter. These measures require qualified specialists to study and analyze data, network traffic and log files received from various information security tools and services in order to detect abnormal behavior, since an attacker who has overcome the outer network perimeter, is almost free in his actions.
Sensor networks, in turn, require autonomy, reliability, fault tolerance and scalability, so the sensor network protection mechanisms are primarily aimed at availability: ensuring stable communication channels, building optimal routes, protecting against DoS attacks. In addition, sensor networks are usually run on low-performance devices and sometimes have strict latency limits (real time data collection and analysis). Given all this, developers of sensor network systems create their own protocols and technologies, which make it impossible to use traditional local network security measures [3].

These factors produce a number of vulnerabilities that an attacker can exploit. First of all, the lack of intruder detection, authentication and encryption mechanisms — an attacker can impersonate a legitimate node of the sensor network, redirect traffic, hack specific nodes, intercept, analyze and modify network traffic, affects the security of sensor networks [4].

As additional protection measures, researchers offer solutions aimed at network exploration protection, for example network steganography and moving target technology. Network steganography conceals the fact of data transfer. The data is hidden in the headers and payload of network packets, the packet-transmission order changes, and some packets are deliberately lost. Network steganography methods do not change the data and do not interfere the functionality of network services. However, network steganography is difficult for implementation and limited in use, because of the limitations on the amount of transmitted data [5].

Moving target technology complicates network exploration by periodically changing the structure and configuration of the network over time. The functioning of the information system is not disrupted, so the attacker has no limits in his actions, but he cannot obtain long-term information about the network [6]. The most effective systems are of the decentralized type, since there is no vulnerable central node. This technology is at the initial stage of development: theoretical solutions and some technical prototypes have been proposed, but researchers still face difficulties with their implementation and application.

These solutions have been tested only for the protection of traditional computer network systems, as a result, they can be inapplicable for sensor networks due to their characteristics.

3. Solution description
The developed method of secure data communication for dynamic network topology is based on moving target technology. Nodes participating in secure data communication move in multicast groups and transmit data using group broadcasting. Each node is simultaneously connected to several multicast groups of secure data communication and redirects the received data to all connected groups, i.e. avalanche routing is used.

When data is transmitted this way, an attacker who intercepts and analyzes the data cannot identify receivers or senders, since the data packets do not explicitly contain their IP addresses. The data packet, regardless of the amount of data transmitted, has a fixed size and is encrypted. Furthermore, participants of the secure data communication switch between multicast groups and the logical structure of the system has a dynamic topology. Retransmission in combination with a fixed packet size does not allow to determine whether the packet is the request or response, and which node is the sender or receiver. As a result, an attacker cannot identify data flows or determine relationships between nodes, as well as cannot obtain long-term information about the logical structure of the system.

At the stage of initialization, each participant node forms a pool of secure data communication multicast group addresses, through which the data is transmitted, according to an algorithm depending on the current date and time. This pool of addresses changes at regular intervals. Next, the node selects two multicast groups and connects to them. At the end of another time interval, which is less than the interval for re-forming the multicast group address pool, the node again randomly selects the multicast groups. The general algorithm for initializing secure data communication is shown in figure 1.
In order to transmit data, each node participating in secure data communication generates a data packet of the structure shown in figure 2, and transmits it to all currently connected multicast groups of secure data communication. All data packets are of the same size, and if the size of transmitted data exceeds the size of the packet, the data is split into several packets. A packet containing the receiver and sender IDs is encrypted with the receiver's public key using a lightweight cryptography algorithm [7]. Nodes connected to receiving multicast groups of secure data communication retransmit this packet to another multicast groups and so on. It should be noted that during retransmission, the packet is modified so that the initiator of data communication could not be identified. It is crucial because otherwise listening to all the network traffic, it would be possible to determine original data sender. Each retransmission generates different packet, and as a result, the sender cannot be identified.

After the retransmission, the node attempts to decrypt the packet header and extract its ID. If the data packet is successfully decrypted, the node processes the packet, otherwise discards it. To ensure that the retransmission is not infinite, each data packet has a lifetime. In addition, the packet is discarded if the...
maximum data packet size is exceeded, or the data packet was previously processed by the node, regardless of whether it is the intended receiver or not.

4. Implementation of the developed solution
The practical implementation of secure data communication based on a dynamic network topology is a daemon that receives UDP datagrams from the MQTT-SN client, encapsulates them in a data packet and transmits them further over the network. MQTT-SN v1.2 is chosen as the application layer protocol, since it supports UDP and is designed to function precisely in a wireless sensor network, in conditions of low bandwidth, poor quality communication channel and low performance of end devices, in contrast to the usual MQTT [8]. NSP Proxy is a software implementation of the solution being developed.

Figure 3. Sensor network diagram.

Figure 3 shows the sensor network diagram. The MQTT-SN network consists of clients, translators and gateways, which in turn are connected to the MQTT broker, normally situated outside the sensor network, by means of a stable and optionally secure TCP connection via MQTT protocol.

The sensor network based on MQTT-SN does not support secure connections: data is transmitted in unencrypted UDP datagrams, there are no authentication mechanisms. The method of secure data communication involves the protection of data by a cryptosystem with a public key. It should be noted that the MQTT-SN client (sensor) only needs to know the public keys of the translator or gateway that forward the data to the MQTT broker. Accordingly, the administrator registers the public and private keys in the device, as well as the public keys necessary for a particular device to receive and transmit data from specific nodes.

Performance characteristics of the developed system: the average bandwidth is 320 kbit/s and the delay is 28 ms. These values were obtained by generating a substantial amount of traffic on a router with a maximum speed of 300 Mbit/s through a wireless connection, the channel width was shared between all participants of the experiment. In a real-world sensor network, such performance characteristics are considered acceptable, a large amount of data is usually not transmitted in a short period of time.

5. Conclusion
The developed method of secure data communication based on a dynamic network topology does not involve the presence of central nodes. It is built on the basis of standard technologies that are supported by most devices operating over a WLAN network (including LAN). The use of this method does not
affect other services or security requirements. The presented method allows to protect from analysis not only the transmitted data, but also the sides of network interaction, and the whole sensor network from the exploration.

References
[1] Boyes H, Hallaq B, Cunningham J and Watson T 2018 The industrial internet of things (IIoT): An analysis framework Computers in industry 101 1-12
[2] Singh P K 2020 Handbook of wireless sensor networks: issues and challenges in current Scenario’s ed Bhargava B K et al. (Cham: Springer Nature Switzerland AG)
[3] Finogeev A G, Nefedova I S, Finogeev E A, Kuang V T and Botvinkin P V 2014 Analysis and classification of attacks via wireless sensor networks in SCADA systems Caspian Journal: Management and High Technologies 1(1) 12-23
[4] Kumar H K and Kar A 2009 Wireless sensor network security analysis Int. journal of computer science & information technology (IJCSIT) 1 1-10
[5] Mazurczyk W, Smolarecz M and Szczypiorski K 2011 Retransmission steganography and its detection Soft Comput. 15 505-15
[6] Zhuang R, DeLoach S A and Ou X 2014 Towards a theory of moving target defense Proc. of the 1st ACM Workshop on Moving Target Defense (Scottsdale: ACM) 31-40
[7] Bhardwaj I, Kumar A and Bansal M 2017 A review on lightweight cryptography algorithms for data security and authentication in IoTs 4th Int. Conf. on Signal Processing, Computing and Control (ISPCC) (Waknaghat: IEEE) 504-9
[8] Stanford-Clark A and Truong H L 2013 Mqtt for sensor networks (mqtt-sn) protocol specification Int. business machines (IBM) Corporation version 1(2)