Attacks and intrusion detection in wireless sensor networks of industrial SCADA systems

V A Kamaev¹, A G Finogeev², A A Finogeev², D S Parygin¹

¹ Volgograd State Technical University, 28, Lenina Ave., Volgograd, 400131, Russia
² Penza State University, 40, Krasnaya Str., Penza, 440026, Russia

E-mail: kamaev@unix.cad.vstu.ru, alexeyfinogeev@gmail.com

Abstract. The effectiveness of automated process control systems (APCS) and supervisory control and data acquisition systems (SCADA) information security depends on the applied protection technologies of transport environment data transmission components. This article investigates the problems of detecting attacks in wireless sensor networks (WSN) of SCADA systems. As a result of analytical studies, the authors developed the detailed classification of external attacks and intrusion detection in sensor networks and brought a detailed description of attacking impacts on components of SCADA systems in accordance with the selected directions of attacks.

1. Introduction

The effectiveness of solving problems of APCS and SCADA systems information security depends mainly on data transmission protection technologies applied to transport environment components.

SCADA systems use a wired or wireless sensor networks as a transport environment for gathering telemetry data and sending commands to executing devices [1].

Because of the transition from wired to wireless network technologies for the construction of sensor networks for gathering telemetry data, the quality of such protection [2] is determined not only by hardware and software solutions for industrial controllers and sensor nodes, but also by the chosen principles of their information interaction in the process of synthesis of network topology, routing determination and data transfer.

Traditional information security measures (the use of sophisticated encryption algorithms, multifactor authentication, antivirus programs, firewalls, etc.) are not always applicable due to the limited computational and energy resources of sensor nodes and WSN as a whole. In addition, manufacturers of industrial automation and execution devices are developing proprietary protocols, which do not allow implementing security technologies using IPSec, SSL, VPN, etc.

If the SCADA system is set in a large area, for example, for monitoring and management of distributed engineering services (heat, water, electricity and gas supplies) [3], then the network of mobile operators (GPRS/3G modem connections) is used as a transport environment with the possibility of public access [4]. This effectively provides a channel for attacks.

Therefore, to build the effective ways of protecting information in wireless sensor networks, it is necessary to analyze the possible types of attacks, methods of their detection, and reasons of system vulnerabilities. Solving these problems is the purpose of this article.
2. Attacks classification

The modern trend towards transport environment of SCADA systems defines the use of self-organizing wireless networks with peer equality, dynamically changing topology, the possibility of network reconfiguration, self-recovery, dynamic routing, etc.

Currently used principles of data transmission in wireless networks provide the possibility of making the four types of impacts: interception, alteration, destruction and code injection. In accordance with the definition of security, all attacks in WSN of SCADA systems can be divided into the following categories [5]:

- Access attacks, which include attempts to gain an unauthorized access to system resources.
- Attacks on privacy, which represent attempts to intercept the data transfer in the transport environment.
- Attacks on integrity, which include the generation and transfer of frames to capture the control over the SCADA system, to cause faults and failures in its work or to prepare other attacks.

We consider the classification of attacks in detail by the directions of impacts and give a detailed description of the main types (see figure 1).

1. Attacks on the sensor network of the SCADA system.
   1.1. Creating active interference in the work area of the SCADA system. To create permanent noises, "white noise" generators are used. They operate on the same frequency as the SCADA system. A source of that noise can be determined using spectrum analyzers and it is possible to stop the attack by locating and eliminating its source [6]. The most dangerous are natural (lightning) or artificial impulse noises, that can lead not only to a system failure, but also damage the sensor nodes and industrial controllers.

   1.2. Attacks on the human-machine interface (HMI) of the SCADA system. An unauthorized access to the web-interface from a mobile device can be carried out in the case of open wireless networks or networks with weak authentication.

   1.3. Attacks on WSN addresses spoofing aimed at Denial of Service (DoS) initiating. We can distinguish two types of such attacks:

   1.3.1. The interception of sensor nodes frames with the purpose of spoofing MAC source and destination addresses, which leads to the failure or malfunction of the SCADA system.

   1.3.2. The replacement of the central coordinator to change the address space of the sensor network configuration.

2. Attacks on sensor network nodes and related devices.
   2.1. Changing the firmware, drivers and software of industrial controllers (PLC – Programmable Logic Controller) and terminal sensor nodes (RFD – Reduced Function Device). The attack is conducted by PLCs and RFDs scanning to identify the opportunities of the preset operating system, firmware, drivers and controllers changing.

   2.2. Injection attacks by spoofing or replacement of the WSN nodes, responsible for collecting and relaying data in the network (FFD – Fully Function Device) to intercept and redirect network traffic. The main purpose of such attack is to redirect the network traffic to the injected or replaced node. We will consider the variety of such attacks:

   2.2.1. Compromising the node by replacing routes confirmation tickets to redirect traffic from the end source-nodes to the injected receiver-node. As a result of such replacement, the real coordinator stops collecting data from the PLCs and sensors, and the dispatch service loses control of technological processes.

   2.2.2. The router (the FFD node) replacement in a sensor network is aimed to violate the correct operation of routing algorithms. The attack can be carried out by:

   - the creation of a "false" tunnel (on the injected router there runs a program that copies retransmitted frames to transfer them to another sensor network, or, conversely, a program of frame transmitting with control commands from another network);

   - setting filters (on the injected router there runs a program that filters and destructs retransmitted frames on the specified criteria or content);
changing routes (on the injected router there runs a program that changes the contents of "Route Record" packets by a given algorithm or at random.

2.2.3. The replacement of the WSN central coordinator to the organization of run-up broadcast storm and to achieve service denial or to power supplies fast discharge.

Figure 1. Classification of attacks by impacts directions.

3. Attacks on the sensor network traffic.

3.1. Listening to data transmission channels. It is produced by network traffic intercepting and decoding with special utilities (sniffers) for the subsequent frames analysis for extracting the required information.

3.2. Attacks with data frames. It is performed by flooding or by generating "false" service or data frames or replacing the contents of captured frames and the subsequent injection into the network [7]. Let us consider the basic options of such attacks.

3.2.1. The injection of a malicious code. It focuses on bringing malfunction to the executing devices, the entire network or on changing the parameters of technological processes. The injection of a self-replicating worm into the network routers leads to infection and transformation of all nodes to the botnet, which nodes generate data frames to increase the network reaction time, producing faults and failures (distributed DoS attack [8, 9]).
3.2.2. Frames filtering and selective broadcast. It is produced by injecting into the network a special type of software or hardware filters that intercept data frames, filter them, and may perform a selective broadcast. The effectiveness of the attack increases with its integration with the "funnel" attack.

3.2.3. Flooding attacks by generating "false" frames (service or data) and broadcasts:
- cloning and broadcast of data frames are performed by intercepting and reproducing repeatedly the same data frames followed by broadcasting in the network to achieve input buffers overflow and network failures;
- generation and broadcast of polling units frames and HELLO-frames to achieve failures of network resources; creating and sending a set of HELLO-frames with non-existent addresses of nodes in the network, it is possible to make an image of a "non-existent" area of the sensor network;
- synthesis of "virtual" source-nodes to broadcast route packets from them (routing DDoS attack); here the weakness of Source-Routing technology is exploited if it is used in centralized SCADA systems with one coordinator and a gateway, namely, the excessive network load with the broadcast routing traffic.

3. The results of intrusion detection in WSN
There are few general traditional techniques aimed to detect attacks in transport network media [10]. All of them include the following procedures:
- identification and validation of a non-standard network traffic;
- periodic inspection of privileges and authorizations for the personnel access to specific information resources of the SCADA system;
- disabling of the unused protocols and services;
- disabling of the remote access and control of the network nodes and applications;
- a periodic scan of network interfaces and drivers;
- timely updating of nodes software from the trusted sources.

There are three ways to detect attacks in networks:
1. Detection by the signatures. The signature defines the characteristics (profiles) of previously committed attacks. During the scanning, a coincidence of signatures is revealed and notification is made. However, this method does not reveal the attack with new (unknown) signatures.
2. Detection of the anomalous behavior. The attack detection occurs when identifying an abnormal behavior of the network node or deviations from its normal operation. The disadvantage of this approach is that an incorrect behaving node may be affected by other factors that are not related to the attacks, such as software, hardware or sensor failure.
3. Combined detection by the specifications. This method combines the two previous ones to reduce their shortcomings. WIDS (Wireless Intrusion Detection System) is a software and hardware solution, which consists of software agents that perform the function of collecting, processing and analyzing network traffic packets. Agents interact with the server, transmitting captured packets to it. The server processes the received data for detecting attack signatures and the anomalous behavior of network nodes, as well as responding to events. Thus, WIDS combines signature and behavioral ways, and relates to the third method. In operation, WIDS performs monitoring and analysis of traffic in the sensor network. Its functionality includes the following standard procedures:
1. The analysis of the WSN topology.
2. The determination of WSN vulnerabilities.
3. The compilation and maintenance of network nodes lists. These lists are generated on the basis of network traffic analysis and retrieval of MAC-addresses of the network nodes from the captured frames. In the future, the resulting lists will actually allow detecting the appearance of new "foreign" potentially dangerous nodes in the network.
4. Detecting and countering attacks in WSN. At the moment, the number of detected attacks in WSN is far less than the number of detected attacks in wired networks, as it is only limited by the OSI
model data link layer traffic analysis. The result of the attack detection is the administrator's notification on potential problems in different ways (via email, SMS messages, etc.) and event logging for auditing.

5. Locating the source of the attack and its suppression. WIDS can use such mechanisms of repression as the implementation of DoS attacks on the attacker’s node, blocking the attacking agent by active network equipment. Locating the source of attacks means the detection of the coordinates of the device that violates security policy by the trilateration, multilateration or triangulation technologies.

6. Control of security policy. It is based on the analysis of the network nodes list in order to detect changes in the policies set by the administrator. An audit can detect the appearance of unauthorized nodes and applications, violations of traffic protection policy.

7. Performing controlled invasion tests through the existing vulnerabilities of the SCADA system and its components by specific exploits.

8. Monitoring of the wireless network capacity and the network response time. In the process of monitoring, WIDS can monitor the physical and data link layers of the network, and identify problems such as:

- overload of a channel, node or network;
- a sharp increase in the number of data frames received by the coordinator, routers and end nodes;
- reduction of radio signals power;
- a sharp increase in the broadcast service or routing frames;
- overlapping with the neighbouring networks;
- reduction of the network bandwidth for no apparent reason;
- a dramatic increase of the route search time;
- a sharp increase of the server applications’ reaction time to client requests;
- an increase of collisions in data channels;
- an appearance of new network nodes;
- reduction of the data transmission rate;
- overload of the network nodes and the network as a whole;
- overflow of nodes’ buffer memory, denial of service, etc.

On the basis of such monitoring results analysis by responsible persons for the information security, the necessary decisions may be made and appropriate operational and long-term measures may be implemented.

4. Conclusion
Despite of rather a large number of possible attacks in wireless sensor networks and SCADA systems, the internal anthropogenic threats are the most dangerous for information security, which include [11]:

- unintentional personnel actions that create the auspicious conditions for external attacks by hackers;
- intentional ignoring the requirements of information security by the staff serving the SCADA system;
- the lack of personnel qualification in the field of information technologies and implementation of information security methods.

Unlike the external intruder, the staff of the enterprise has great opportunities for attacks to infect and spread a malicious code on the sensor network. Information security problems are often caused not so much by external attacks, but by the staff non-compliance of regulations and rules of the enterprise information security policy.

Managers and other staff of the enterprise may ignore their duties and in their "free" time are busy with "surfing" the Internet, social networking, and playing computer games.
It may result in an unauthorized PC infection by computer viruses, Trojan horses and worms, which then may penetrate into the sensor networks. This explains the fact that viruses and worms like Stuxnet are often present in industrial systems, and the fact that their presence is normally hidden by staff and managers, as the disclosure of this information will lead all the staff and management to the detailed inspection and then to the subsequent negative consequences for them. In addition, the finding of the infection in the SCADA system may cause a need of hard reset to clean the virus and will stop the most of the enterprise’s processes, but it is not always feasible from the economic standpoint.

The lack of qualifications of the personnel, who work with PLCs and SCADA systems, also requires the involvement of outside experts to identify and correct software changes in controllers, because after cleaning the system, it is necessary to be ensured that the programs and settings in the controllers correspond to the values required for the proper functioning of the industrial automation complex.

It is well known that the human factor is the main reason of deviations from the normal operation status in various technical systems. This requires special attention to the establishment and maintenance of appropriate technical regulations.

Acknowledgments
The reported study was funded by RFBR according to research projects No. 16-07-00031_a, No. 15-07-01720_a, No. 16-37-50017_mol_nr, No. 15-57-54033_Vet_a and the Russian Ministry of Education in scope of the base part (project 2586 of task N 2014/16).

References
[1] Tyulkina E, Vassiliev P, Janovsky T and Shcherbakov M 2014 Communications in Computer and Information Science (Springer IPS) 466 542–555
[2] Kravets A G, Bui N D and Al-Ashval M 2014 Communications in Computer and Information Science (Springer IPS) 466 371–382
[3] Kamaev V, Finogeef A, Finogeef A and Shevchenko S 2014 Proc. 11th Joint Conf. Knowledge-Based Software Engineering (Springer International Publishing Switzerland) pp 1–15
[4] Finogeef A G, Dilman V B, Finogeef A A, Nefedova I S and Finogeef E A 2014 Mater. Int. Sci.-Practic. Conf. on Innovative information technologies ed S U Uvaysov (Moscow: HSE) part 3 pp 109–116
[5] Frolov S G and Demin A U 2016 Proc. 3d Int. Conf. on Information technologies in science, management, social services and medicine (Tomsk: TPU) pp 74–76
[6] Sokolov A, Tyukov A, Sadovnikova N, Zhuk S, Khrzhanovskaya O and Brebels A 2015 Communications in Computer and Information Science (Springer IPS) 535 462–473
[7] Banokin P I 2016 Proc. 3d Int. Conf. on Information technologies in science, management, social services and medicine (Tomsk: TPU) pp 106–109
[8] Beitollahi H and Deconinck G A 2011 The 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-11) pp 11–20
[9] Beitollahi H and Deconinck G 2012 Analyzing Well-Known Countermeasures against Distributed Denial of Service Attacks Elsevier J. of Computer Communications 35(7) 829–841
[10] Beitollahi H and Deconinck G 2012 Elsevier J. of Computer Communications 35(7) 829–841
[11] Bolshakova O N and Chusavtina G N 2016 Proc. 3d Int. Conf. on Information technologies in science, management, social services and medicine (Tomsk: TPU) pp 122–126