VERSITA
Information Technology and Management Science
doi: 10.2478/v10313-012-0021-8
2012 /15

The Use of Intrusion Detection Systems Based on the Network Behaviour Analysis in SCADA Networks

Aljona Skorobogatjko[1], Pjotrs Dorogovs[2], Andrejs Romanovs[3], [1-3]*Riga Technical University*

***Abstract* – Process Control Systems (PCS) is the set of systems that remotely controls and receives sensory signals. Supervisory Control and Data Acquisition System (SCADA System), usually referred to as a dispatch control system, is the subset of PCS that controls systems over a large distance [1]. Security assurance of such systems against modern cyber threats has become an extremely topical issue in recent years. The paper describes possible security solutions, as well as gives an overview on the SCADA network modelling possibilities.**

***Keywords* – information security, intrusion detection, security of SCADA network, modelling of SCADA network**

I. Introduction

Monitoring, control and data acquisition (Supervisory Control and Data Acquisition – SCADA) systems form a critical infrastructure related to energy supply utilities, water and wastewater treatment plants, as well as large-scale transport systems, such as cross-border railways. Nowadays, SCADA networks are increasingly exposed to cyber attacks. The problem has become extremely topical taking into account expansion of SCADA networks and usage of global networks for dispatching purposes.

Process Control Systems (PCS) is the set of systems that remotely controls and receives sensory signals. Supervisory Control and Data Acquisition System, usually referred to as a dispatch control system, is the subset of PCS that controls systems over a large distance [1]. SCADA systems form a critical infrastructure that connects power supply equipment, water and sewage drainage systems, as well as large-scale transport systems, for example, cross-border railways.

Most of the SCADA and other process management systems that are currently used by companies were developed several years ago, long before the global and private network or the emergence of the personal computers. That is why at the time of implementation of dispatching systems it was not necessary to include any cyber security features. At that time, a good SCADA system security meant physical access limitation to the network and the management and control of hardware. System designers thought that if the SCADA system is adequately insulated from the physical access of any unauthorized person and can be accessed only by authorized personnel it is secured, and most likely will not be compromised. This law does not work any more.

II. Overview

Nowadays, the dispatch control system used in one of Latvian largest energy production companies has functionality that completely satisfies the proposed requirements for its use. However, the question of network security improvement always remains topical. Due to the fact that production and distribution of electric power is the main part of the state critical infrastructure, the dispatch control system may be attacked by “cyber-terrorists”. Such attackers use all possible and hardly available means and information sources to obtain detailed comprehension of SCADA systems, their possible vulnerability, as well as defects in dispatch control system security of a particular company. Because of the complexity of different system network, engineers frequently cannot prevent additional load that threatens the safety of systems. The purpose of this paper is to improve the total SCADA system safety level using modern solutions in information technology.

Network security solutions are firewalls, antivirus software, Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs), Network Behaviour Analysis (NBA), and Network Behaviour Anomaly Detection (NBAD) systems. IDS detects the attack of network or computer system and follows the data that streams from one computer system to another. IPS prevents the attack of a computer network or computer system preventing data takeover or damages [2] (Fig. 1). NBA system analyzes data streams during the data transfer time in computer systems and offers results of effective analysis in real-time. Network Behaviour Anomaly Detection system identifies anomalies and reveals unreliable processes on the basis of information about the calculated optimal data stream during the data transfer [3].

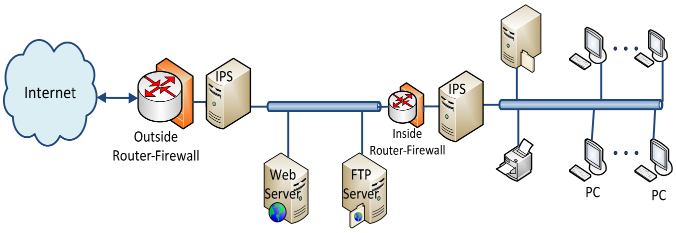


Fig. 1. Displacement of intrusion protection system

III. Modern SCADA Network Security Concepts

One of the most mysterious areas of information security is the security of industrial systems. There is not any other area of information security, which includes so many myths, mistakes, misconceptions and lies. Very high rate of industrial system security also increases the level of secrecy. If the trade secret disclosure may bring great losses to the company, the electricity production management going into "the wrong hands" can kill thousands of people.

Misunderstandings are the main barriers for network security professionals to implement the best possible information security strategies. Security of SCADA systems can be divided into three main misconceptions: SCADA system is located in completely separated networks, connections between SCADA systems and other corporate networks are protected with strong access controls, and SCADA systems require specialized knowledge, which makes them less susceptible to network attacks [5].

A. SCADA Systems Located in a Separate, Stand-Alone Network

Most of the SCADA systems were built before and often in isolation from other corporate networks. As a result, IT managers raised complaints that these systems were not accessible from corporate network or remote access points.

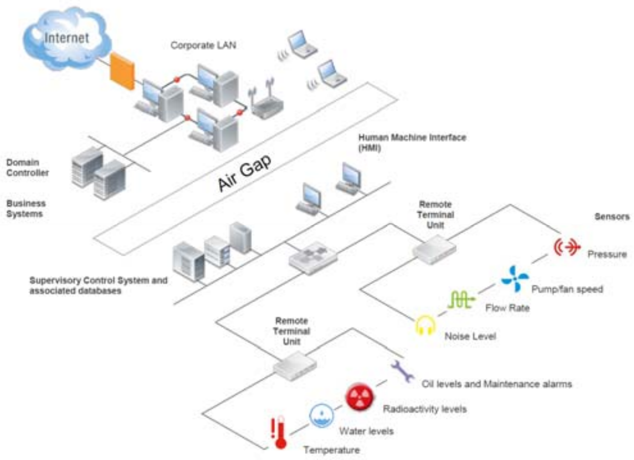


Fig. 2. SCADA network

Now, thanks to two changes in the best practices of information management, dispatch control system networks and enterprise information technology systems are often connected. First, remote access to SCADA brings engineers an opportunity to connect to the system using a variety of programs and processes for the management and control through corporate networks (Fig. 2 shows that the SCADA network is connected to the corporate network, which in turn is linked to an external network).

Second, many utilities make connections between the corporate and SCADA networks to gain instant access to critical data on the overall system and individual operation status that is necessary for the business important decision making. Often, these connections are established without awareness of any of possible security risks. In fact, corporate network security strategy rarely takes into account the fact that access to these networks provides access to the dispatching system and its control.

B. SCADA Systems and Networks Protected with Strong Access Control

Many enterprise networks and SCADA system connections need to be consistent with a number of communication standards. Because of the difference in complexity of the systems that are being integrated, network engineers often fail to prevent additional burdens that threaten the security of the system.

As a result, the corporate network access control, protecting SCADA systems from unauthorized access, usually is minimal. This is largely due to the fact that network administrators simply forget about any open access point and do not control its usage. Although international standards and specifications recommend making use of an internal firewall, intrusion detection system and strong password policies, no utility program is able to completely protect all entry points of a dispatching system.

C. SCADA Systems Require Specialized Knowledge

The assumption that all SCADA system attackers lack the ability to access information on the development and operation of a system is incorrect. Due to the fact that many national engendering communication network management systems to some extent are part of country’s critical infrastructure they are possible targets for cyber-terrorist attacks. Such attackers are highly motivated and well funded; they are the best of the world's hackers. They will use all available sources of information to gain a detailed understanding of SCADA systems and their potential vulnerabilities, as well as probable network security bugs of the used dispatching system.

A growing number of attacks, the constant progressive threats and new vulnerabilities in SCADA networks can bring a national disaster.

IV. Analysis of Typical Attacks and Security Solutions

Typical attacks aimed at SCADA systems using standard hardware and software features are the following:

- malicious code such as viruses and worms;
- unauthorized access to the company's business critical data;
- unauthorized change and transfer of this data to other people.

Three network protection levels for solution of SCADA system network security can be distinguished:

- physical protection level. At this level, physical access to SCADA systems and other network hardware is controlled;
- intra-company level. At this level, staff access to certain information is regulated;
- an external level. At this level, corporate information resources and technologies that can be accessed by an external network user, for example, a customer, are determined.

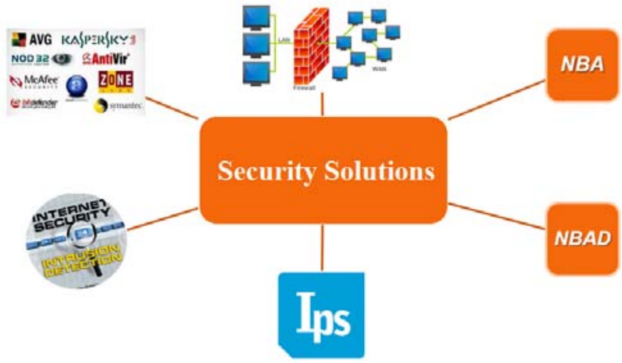


Fig. 3. Network level security solutions

The external network protection level includes a broad range of issues related to electronic transmission of information from one place to another. Lack of control of this level of SCADA system security can bring greatest losses for the business itself, as well as create national disasters [4].

Theoretically, data transmission can be established both between systems in different continents, and between the company's internal systems. Thus, data becomes vulnerable to various types of network failures that threaten the confidentiality and integrity of the transmitted data. However, many of these threats can be reduced or eliminated by appropriate means. Network security solutions are designed for detection and prevention of errors in the transmitted information, as well as for correction of information that have been intentionally amended. Fig. 3 shows a diagram of external network protection level security solutions.

Network invulnerability assurance is a continuous process, where new threats arise all the time. However, many network security solutions consume too much system resources, which may disturb real time operation of the SCADA system.

One of the main reasons behind monitoring and storing of network activity logs is the physical and logical level intrusion detection and prevention. In case, unusual activity warning and comparison with the previously collected data solution are implemented, it is easier to detect real-time attacks and prevent them in the SCADA system.

In particular, at the logical level, where an attack could bring losses in seconds, automatic equipment should be equipped with intrusion solution tools. Such tools can be divided into two main categories: Intrusion Detection Systems – IDSs and Intrusion Prevention Systems – IPSs. IDS works exactly as a monitoring and alerting tool, which generates alerts on a possible attack the protected system is subject to or on the detection of an unknown activity. IPS generally works with IDS generated alerts. It analyses them and initializes protective actions. As a counter measure to the detected attack on the network IPS may even reject the entire traffic of the attack source.

V. Modelling of the SCADA Network

Nowadays, security studies are being used while developing a new system or the upgrade project of the already used system is being implemented. A typical starting point of a security survey is the current situation analysis and the identification of safety issues. The next step is the development of a real model of the system at such level of abstraction so that security issues are explored without overcoming inappropriate wasting of time and financial resources. In order to break the attacker's plans and the impact of the attack, protective measures are applied.

Assessment of security level of the SCADA network can be imagined as a three-step approach, similar to the above-described modelling of system attacks and countermeasures.

The first step is the modelling of the computer network under normal conditions, when it is not under any type of attack. During modelling, a number of metrics are being generated that later will serve as a basis for comparison. For example, the average packet delivery success or the specific network segment throughput can be estimated.

Model of an attacked computer network uses the model developed in the previous step in addition to the attacker's model. In both steps, metrics of simulation results are compared, and the impact of the attack is determined.

Then the attack impact analysis and security standards recommendations are used to develop a security mechanism for future prevention of such an attack. Later, the model of defence mechanism is added to the model of previous step attempting to protect a computer network from the modelled attack. Then simulation result metrics of the second and third steps are compared, and conclusions regarding effectiveness of the mechanism used for protection are drawn.

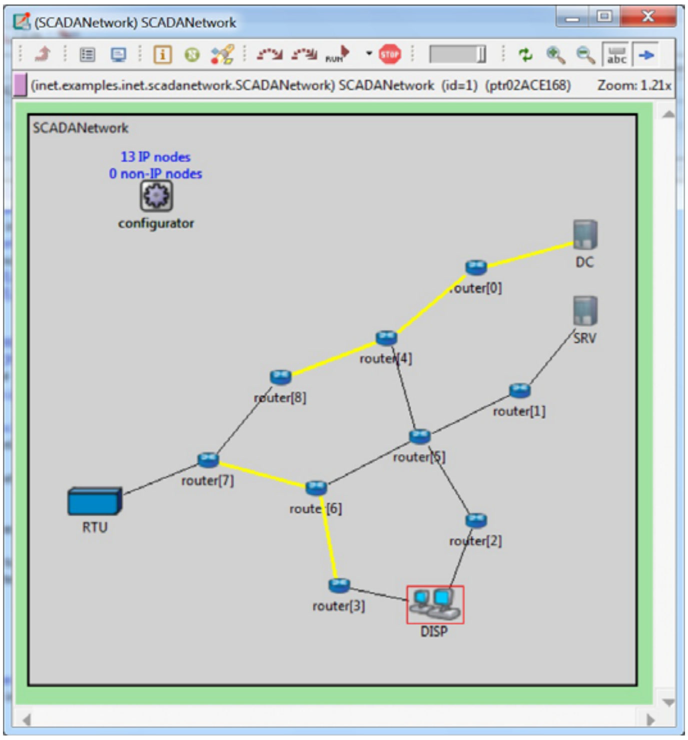


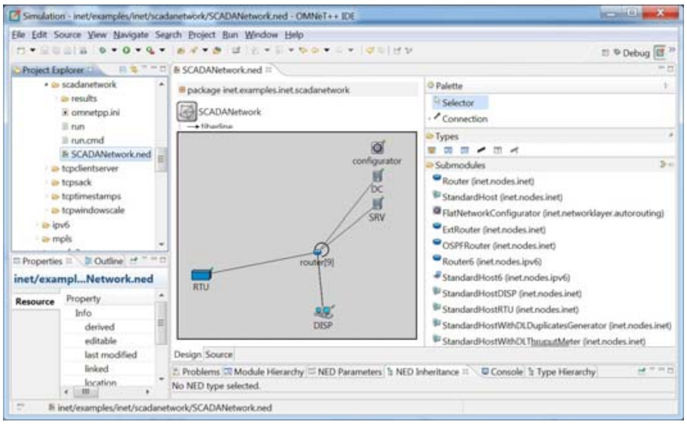
Fig. 4. The model of the SCADA network

While most attacks and security measures can be modelled using simulation, there are also a number of safety problems that cannot be modelled, for example, the usage of social engineering by the attacker to learn from a SCADA controller a way to seamlessly infiltrate dispatchers' work place.

Nowadays, one of Latvian energy production companies does not use any kind of intrusion detection or intrusion prevention systems; however, the company shows its interest in functionality of such systems. For this reason, the SCADA network of this company has been modelled based on the obtained information.

To meet the requirements, the usage of special network modelling software is possible. For example, Boson Netsim, OMNeT++, OPNET Modeler or SSFNet. OMNeT++ and SSFNet are open source software, but others offer only demo-versions for free. OMNeT++ has the graphical user interface that is not available in SSFNet. That is the reason why the OMNeT++ modelling tool has been chosen for the development of a model.

In order to develop the SCADA network model as in Fig. 4, OMNeT++ has been expanded with the communications network modelling package – INET Framework. The model displayed in Fig. 5 has been developed using additional INET Framework modules such as StandardHost, Router and FlatNetworkConfigurator. The StandardHost module has been used to simulate Data Centre (DC), Server (SRV), dispatcher work places (DISP) and remote terminal units (RTU). All 9 routers have been simulated using Router modules, and automatic network configuration has been implemented using FlatNetworkConfigurator module.


Simulation - inet/examples/inet/scadanetwork/SCADANetwork.ned - OMNeT++ IDE
File Edit Source View Navigate Search Project Run Window Help
Debug
Project Explorer
scadanetwork
results
omnetpp.ini
run
run.cmd
SCADANetwork.ned
tcpclientserver
tcpsack
tcptimestamps
tcpwindowscale
ipv6
mpls
SCADANetwork.ned
package inet.examples.inet.scadanetwork
SCADANetwork
configurator
DC
SRV
router[9]
RTU
DISP
Palette
Selector
Connection
Types
Submodules
Router (inet.nodes.inet)
StandardHost (inet.nodes.inet)
FlatNetworkConfigurator (inet.networklayer.autorouting)
ExtRouter (inet.nodes.inet)
OSPFRouter (inet.nodes.inet)
Router6 (inet.nodes.ipv6)
StandardHost6 (inet.nodes.ipv6)
StandardHostDISP (inet.nodes.inet)
StandardHostRTU (inet.nodes.inet)
StandardHostWithDLDuplicatesGenerator (inet.nodes.inet)
StandardHostWithDLThruputMeter (inet.nodes.inet)
Properties
Outline
inet/exampl...Network.ned
Resource
Property
Info
derived
editable
last modified
linked
location
Design
Source
Problems
Module Hierarchy
NED Parameters
NED Inheritance
Console
Type Hierarchy
inet/examples/inet/scadanetwork/SCADANetwork.ned

No NED type selected.

Fig. 5. The SCADA network model in the OMNet++ environment

VI. Conclusions

The conceptual model of the SCADA network has been created, and, as a result, the SCADA network model has been developed using the OMNeT++ simulation tool.

Later, the imitation of attacks and the extension of developed model with necessary defence mechanisms have been performed.

The analysis of the results of imitation has shown that the network behaviour analysis system for prevention of possible cyber attacks will be the best-suited option for the SCADA systems to improve the overall security level of the whole system.

During the analysis of the results, some recommendations on how to improve the SCADA network safety have been offered.

References

[1] D. Bailey, E. Wright, Practical SCADA for Industry. Elsevier, 2003.

[2] S. Jacobs, Engineering information security: The application of systems engineering concepts to achieve information assurance. Wiley Publishing, 2011.

[3] J. Andress, The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Elsevier, 2011.

[4] Vacca J. Network and System Security. – Elsevier, 2010. – 668 p.

[5] Krutz R. Securing SCADA Systems. – Wiley Publishing, 2006 – 218 p.

Aljona Skorobogatjko is a master student at the Department of Modelling and Simulation, Riga Technical University (Latvia). She received her Bachelor Degree in Information Technology from Riga Technical University in 2012. Her Bachelor Thesis on SCADA network security received special support from the Latvian local energy producing company and was among laureates of the Latvian best theses in the field of Information Technology in 2012.

Her professional interests include designing and modelling of network security systems. She has participated in a number of international scientific conferences. E-mail: alona.skorobogatjko@rtu.lv.

Pjotrs Dorogovs is a doctoral student at the Department of Modelling and Simulation, Riga his Technical University (Latvia). He received Bachelor Degree in Information Technology from Riga Technical University in 2005. He obtained his Master Degree in IT Project Management (MSc.ing.) from Riga Technical University in 2008. His research interests include IT security and IT governance. Currently, he is an Acting Deputy Chief of the Information Centre of the Ministry of the Interior of the Republic of Latvia. Since 2006 he has been participating in monthly large-scale IT system management forum taking place mostly in Brussels organized by the European Parliament. He has managed the implementation of some large-scale IT systems for the Latvian law-enforcement authorities including putting into production the Schengen information system. He is a member of the IEEE. He has participated in several international scientific conferences and research projects with scientific publications in the field of ICT. E-mail:pjotrs.dorogovs@rtu.lv.

Andrejs Romanovs, Dr.sc.ing, Associate Professor and Senior Researcher at the Information Technology Institute, Riga Technical University. He has 25 years of professional experience in teaching postgraduate courses at RTU and developing more than 50 industrial information systems as IT project manager.

His professional interests include modelling and design of management information systems, information systems for healthcare, IT security and risk management, IT governance, integrated information technologies in business, as well as education in these areas.

A.Romanovs is a senior member of the IEEE and LSS, Council Member of RTU ITI, author of 2 textbooks and more than 30 papers in scientific journals and conference proceedings in the field of Information Technology. He also participated in 25 international scientific conferences, as well as in 7 national and European-level scientific technical projects. E-mail: andrejs.romanovs@rtu.lv.

Aļona Skorobogatjko, Pjotrs Dorogovs, Andrejs Romānovs. Uz tīkla uzvedības analīzes bāzēto telaušanas noteikšanas sistēmu izmantošana SCADA tīklos
Procesu vadības sistēmas (Process Control Systems – PCS) ir sistēmu kopums, kas attālināti kontrolē un saņem sensoru signālus. Uzraudzības vadības un datu apkopošanas sistēmas (Supervisory Control and Data Acquisition system – SCADA sistēma), ko parasti sauc par dispečeru vadības sistēmām, ir PCS sistēmu apakškopa, kas nodrošina citu sistēmu attālināto kontroli. Šādas uzraudzības, kontroles un datu apkopošanas sistēmas veido valsts kritiskās infrastruktūras, kas ir saistītas ar energoapgādes piegādes pakalpojumiem, ūdens un notekūdeņu attīrīšanas iekārtām, kā arī liela mēroga transporta sistēmām, piemēram, pārrobežu dzelzceļiem. Šādu sistēmu drošības nodrošināšana pret mūsdienu kiberdraudiem pēdējos gados kļuvusi ļoti aktuāla, it īpaši, ņemot vērā, ka lielākā daļa no SCADA un citu procesu vadības sistēmām, kas pašlaik tiek izmantotas uzņēmumos, tika izstrādātas pirms vairākiem gadiem, ilgi pirms globālo un privāto tīklu vai personīgo datoru parādīšanās. Tieši tāpēc šo sistēmu implementācijas laikā netika izvirzītas nopietnas prasības sistēmu drošības pasākumiem. Darbs apraksta iespējamos drošības risinājumus, kā arī sniedz pārskatu par SCADA tīkla modelēšanas iespējām. Darba mērķis ir uzlabot kopējo SCADA sistēmas drošības pakāpi, izmantojot modernus informācijas un komunikācijas tehnoloģijas risinājumus. Darba izstrādes laikā tika izpētītas SCADA tīkla drošības problēmas un meklētas iespējamās datu drošības nodrošināšanas tehnoloģijas, tādēļ tika apskatīti drošības standarti un izanalizētas uz anomāliju noteikšanu un ļaunprātīgu darbību atklāšanu bāzētas tīkla drošības nesankcionēto darbību atklāšanas un pretielaušanās sistēmas. Ir izstrādāts SCADA tīkla modelis ar OMNeT++ modelēšanas līdzekļa palīdzību, tajā tika imitēti vidutāja uzbrukumi un drošības mehānismi. Izstrādātās funkcionālās prasības tīkla uzvedības analīzes sistēmai var kalpot kā palīginstruments valsts mēroga elektroenerģijas ražošanas kompāniju speciālistiem pareiza drošības risinājuma izvēlei.

Алёна Скоробогатько, Пётр Дорогов, Андрей Романов. Использование систем обнаружения вторжений, основанных на анализе поведения сети в индустриальных сетях SCADA
Системы управления технологическими процессами (Process Management Systems – PCS) - это комплекс систем, позволяющих вести удаленное управление процессами и получать и обрабатывать сигналы с сенсоров. Системы диспетчерского управления и сбора данных (Supervisory Control and Data Acquisition system – SCADA-системы), как правило, называют наземными системами контроля и управления, по сути, являются подмножеством PCS систем и обеспечивают дистанционное управление других систем. Такие системы мониторинга, диспетчерского управления и сбора данных составляют государственную критическую инфраструктуру, связанную с поставкой энергетических услуг, управлением поставками воды, содержанием очистных сооружений, а также с крупномасштабными транспортными системами, такими как межгосударственные железные дороги. Обеспечение безопасности таких систем от кибер-угроз в последние годы стало очень актуальным вопросом, учитывая, что большинство SCADA и других систем управления технологическими процессами, которые в настоящее время используются на предприятиях, были разработаны несколько лет назад, задолго до появления глобальных и частных сетей или персональных компьютеров. Работа описывает возможные решения в области безопасности, а также предоставляет обзор возможностей моделирования сетей SCADA. Целью работы является улучшение общей безопасности систем SCADA, используя современные средства информационных технологий и возможностей коммуникации. Во время подготовки работы были изучены проблемы сетевой безопасности SCADA систем и найдены возможные технологии обеспечения безопасности. Для этого были рассмотрены стандарты безопасности и проанализированы системы обнаружения и предотвращения вторжений, основанные на анализе сигнатур и аномалий в поведении пользователей и приложений сети. Используя среду моделирования OMNeT++, была разработана модель SCADA сети, имитированы атаки «человек посередине», затем модель была дополнена механизмами защиты. Функциональные требования к системе анализа поведения сети, разработанные автором научной работы, помогут специалистам отдела стратегического развития при выборе системы защиты SCADA сети.