Analysis of SCADA System Vulnerabilities to DDoS Attacks

Jasna D. Markovic-Petrovic[1], Mirjana D. Stojanovic[2]

Abstract – **Several factors have contributed to the escalation of risks specific to novel control systems, including the network architecture, adoption of standardized technologies with known vulnerabilities and connectivity of control systems to other networks. This paper considers SCADA (Supervisory Control And Data Acquisition) system vulnerabilities as well as securing the infrastructure of power utility information-telecommunication systems. We first present a concept of SCADA architecture in the hydropower plants. The simulation model assumes Distributed Denial of Service (DDoS) attack to SCADA system. A comprehensive simulation points to SCADA performance deterioration under DDoS attack. Possible security solutions have also been discussed.**

Keywords – **Network security, Distributed Denial of Service, SCADA, Simulation.**

I. INTRODUCTION

Important role of the electric power system raises the need for modern telecommunication network that will fully meet the requirements of such companies. This system has to provide availability of correct and timely information in order to plan production, efficient utilization of energy resources, remote controlling of facilities for production, transmission and distribution of electric power, reporting and successful operation of electric power system.

The architecture of modern ICT (Information and Communications Technology) networks for utilities assumes connectivity between a corporate and the SCADA system network. The design of these networks should enable provisioning of operating and corporate telecommunications services along with meeting a certain number of technical requirements and features. Operating services include: remote control, teleprotection, operating telephony and operating video. All of these are directly or indirectly connected with the technological procedure of power generation in electric power systems. Due to their significance, strict requirements for reliability, availability and delay have been defined for these services [1]. Operating services do not generate variable and unpredictable intensity of traffic. Corporate services are transfer of corporate data, telephony, multimedia services. Requirements such as delay, reliability and availability are far less strict, while the dominant one is the requirement for enough network bandwidth.

[1]Jasna D. Markovic-Petrovic is with the CE Djerdap HPP Ltd., Kralj.Marka 2, Negotin, Serbia, E-mail: jasna.markovic@djerdap.rs

[2]Mirjana D. Stojanovic is with the Faculty of Transport and Traffic Engineering University of Belgrade, Vojvode Stepe 305, Belgrade, Serbia, E-mail: m.stojanovic@sf.bg.ac.rs

Advanced ICT networks for utilities assume that the Internet Protocol (IP) technology is used to integrate both operating and corporate telecommunication services. Such networks may have a number of vulnerabilities and weaknesses that are known to malicious users. A starting point for securing these networks is to analyze different kinds of attacks and their consequences to network performance. Four basic categories of attacks on the information system infrastructure have been identified in [2]: (1) DNS (Domain Name System) hacking; (2) routing table poisoning; (3) packet mistreatment and (4) Denial of Service – DoS. Several attacks on industrial control systems have been noted worldwide such as the attacks on the ICT systems in power generation [3], [4]. Security management is a continuous process, which needs to provide safe approach to information and resources. The network requires: securing the confidentiality and integrity of information, user authentication, access control, service availability and non-repudiation. Network security consists of prevention, detection and reaction to the attack. Security management assumes defining a set of policies and choosing the corresponding security mechanisms. These activities are a constituent part of the risk management process. The basic steps are value and criticality analysis, vulnerability analysis, threat identification, risk analysis, risk assessment, security safeguards selection and implementation, development of contingency plans, and effectiveness reviews [5].

The objective of this paper is to provide the analysis of the SCADA system vulnerability, particularly regarding DDoS attacks. For that purpose, comprehensive simulations have been carried out, assuming a typical IP-based SCADA system architecture within a power plant. Directions towards SCADA security solutions have also been outlined.

II. SCADA SYSTEMS VULNERABILITIES

The peculiarity of the ICT system in power utility is the integrated system for remote control and management of power facilities where SCADA is also included. Fig. 1 shows the "rings of defence" of the corporate and SCADA networks. Attacks on the SCADA system can be external, via the Internet through the corporate network, or internal which can influence from the corporate network or the SCADA system from the RTU (Remote Terminal Unit) level or the application level. The development of a corresponding security strategy includes an analysis of multiple layers of the corporate network and the SCADA system architecture (this includes firewalls, proxy servers, operating systems, applications, communications, policies and security procedures) [6].

978-1-4799-0902-5/13/$31.00 ©2013 IEEE

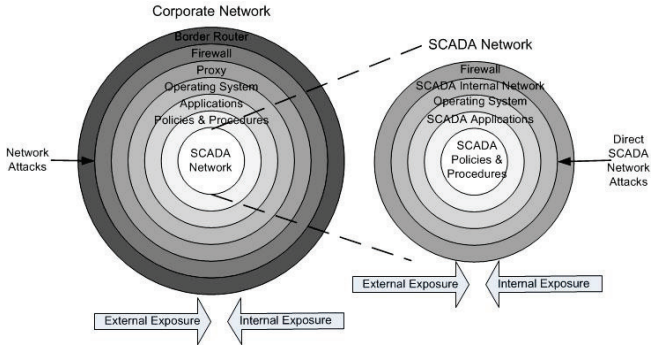

Fig. 1. Relationship between corporate and SCADA networks

Remote control is an adopted approach of monitoring generation and working parameters in power plants. The SCADA system provides timely and accurate information on the process and condition of power facilities which contributes to an efficient, reliable and safe control and management as well as to optimisation of the production process, transmission and distribution of power. This service is characterised by a transmission of data in real time. In general, the SCADA system consists of three hierarchical layers: (1) the process level; (2) the communication system and (3) the central system [6], [7]. Fig. 2 shows a schematic conception of the SCADA system architecture in a selected power plant.

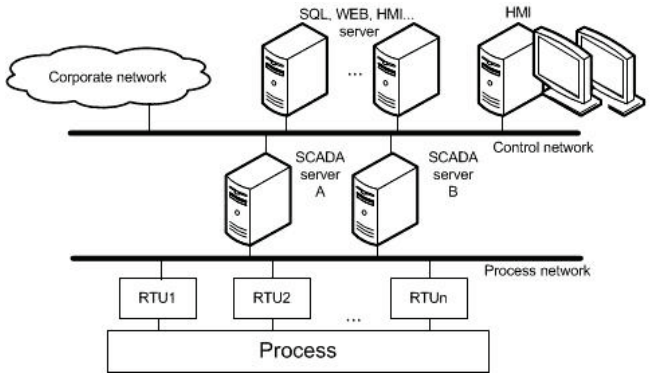

Fig. 2. SCADA block diagram

Advanced ICT networks, which are implemented in the SCADA systems, differ from the initial dedicated networks due to the possibility of integration in the corporate network. The tendency to set up a unique communication infrastructure for transmission of different types of data has led to the breakthrough of the Ethernet and TCP/IP technologies into the SCADA systems. These technologies enable access to the SCADA systems data through Web browsers. This way the data are available even to users who are not located within the local computer network and do not own any SCADA software. The use of the mentioned open standards causes vulnerability of the SCADA system [6].

Over the last decade there have been several successful attacks on industrial control systems worldwide. There has been an increase in the SCADA system vulnerability due to: (1) the adoption of standardised technologies with known vulnerabilities; (2) connectivity of control systems to other networks; (3) constraints on the use of existing security technologies and practices; (4) insecure remote connections and (5) widespread availability of technical information about control systems.

Malicious users use well-known weaknesses of the ICT system but also the specific vulnerabilities within the SCADA system security mechanisms such as: (1) operating systems vulnerabilities; (2) frequently neglected authentication; (3) remote access, which enables system configuration; (4) connectivity to the other networks; (5) the use of wireless connections; (6) the absence of antivirus software with the purpose of rational use of processor resources due to the work in real time; (7) the absence of any kind of the Intrusion Detection System; (8) insufficient experience of employees and (9) insufficient physical security of places where SCADA system devices are located, which are quite often geographically dispersed and without attendance.

III. Simulation and Results

We use the OPNET (Optimized Network Engineering Tool) IT Guru Academic Edition [8], which represents a virtual network environment for modelling, simulation and analysis of different network topologies. OPNET enables simulation of characteristics of the modelled network, statistical analysis as well as a graphic display of the obtained results.

The simulation is carried out via two scenarios: (1) a model without an attack on the network infrastructure and (2) a model during the DDoS attack. In the first scenario, the simulation model is created by defining a network topology and a traffic model under non-attack conditions. By repeating the first scenario the other one appears where the simulation traffic model is extended by a traffic profile which simulates a DDoS attack based on the intensity of generated traffic and not on its content. In DDoS attacks, the attacker can generate traffic similar to legitimate traffic which makes defence mechanisms more difficult. By using multiple sources the attack force becomes increased. A typical DDoS attack involves two phases [9]. In the first phase, the attacker uses vulnerabilities of the available systems and takes control over them thus making them “zombies”. In the second phase, the attacker sends commands thus giving instructions to attack the victim. The attacker spoofs the IP address of the traffic source thus disabling identification of the attack source. The simulation model assumes that the malicious user has already taken control over the “zombie” network, which is located inside the corporate network connected to the Internet. In both scenarios the simulation lasts 150 seconds, while the DDoS attack in the 2nd scenario starts at the 100th second.

The network consists of the two subnetworks. The first one represents the corporate network, while the second subnetwork includes nodes of the remote control system and power plant management. The SCADA system network is modelled without aggregation and is made up of a station part of the network with servers and HMI (Human Machine Interface) computers for visualisation of the process and a process part of the network with remote stations for management of hydro aggregates and additional systems of the plant. SCADA servers have two network interfaces (the object is created by using Device Creator options). Fig. 3

shows a part of the topological model representing the system for control and management in the plant. The corporate network includes 50 clients, out of which 20 clients stand for the "zombie" network.

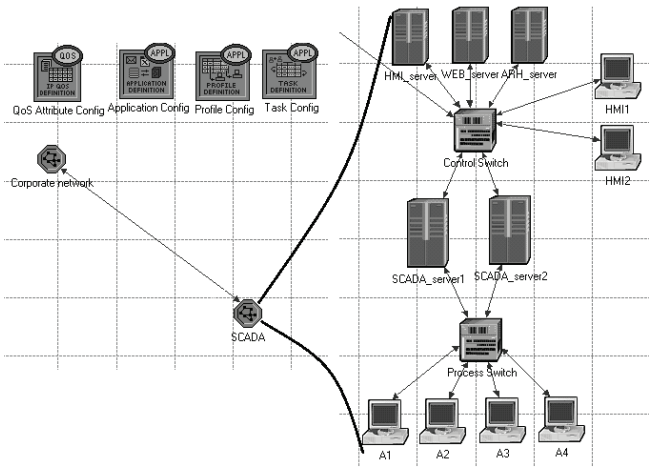

Fig. 3. Simulation model: Topology of the SCADA network

There are three streams of traffic in the simulation model: (1) within the network of systems for remote control and management; (2) between the corporate network and the SCADA systems and (3) the traffic resulting from DDoS attacks.

There are three profiles based on the FTP application which uses a reliable transport service implemented through TCP protocols that are defined for SCADA traffic: (1) forwarding the measurement results from the facility towards the dispatcher centre (the time of event repeating is a constantly short period, while the amount of data matches the uniform distribution within lesser values); (2) the exchange of alarm signals and commands between the dispatcher centre and the facilities (generated traffic is based on the Poisson distribution); (3) the exchange of dispatcher reports between the SCADA systems (the repeating time is a constantly longer period, while the amount of data matches the uniform distribution – larger files).

The other group of traffic features: (1) Web applications that help to obtain a visual display of the process and the needed reports on the corporate network clients; (2) transmission of data towards superior and other remote control centres and (3) access to servers for the needs of configuration from the corporate network clients. The traffic is modelled by using standard applications (Database, FTP, Web) in seven different profiles.

The UDP flood option is selected for the DDoS attack, while malicious traffic has been modelled by using a user-defined application. For this purpose, a task has been defined by using the Task Configuration object, where the traffic flow exists only from the source towards the destination and is based on the UDP transport protocol. The target of the attack is the SCADA server.

The WFQ (Weighted Fair Queuing) packet scheduling discipline is applied at each node. The traffic in the user queue is classified in four priority classes according to the ToS (Type of Service) field value, while the remote control operating service is given the highest priority.

Such a simulation model offers possibilities of thorough analysis of network performances. Remote control service sets up certain requirements for performances. This is not a time-critical service so that a 1s delay is permitted, but it does set up strict requirements for service availability which needs to be higher than 99.98% [1].

Fig. 4 shows a graphic display of outgoing traffic on the router interface towards the SCADA network. The level of victim's processor utilization is depicted in Fig. 5. The graphics refer to the initial moment of the DDoS attack. The attack's influence on the remote control operating service is depicted in Fig. 6, through the packets dropped from the corresponding queue. Fig. 7 illustrates the TCP packet delay on the SCADA server.

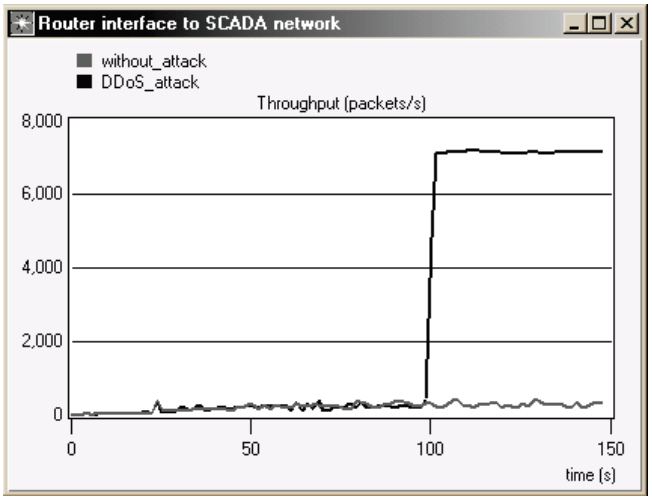

Fig. 4. SCADA network: Received traffic

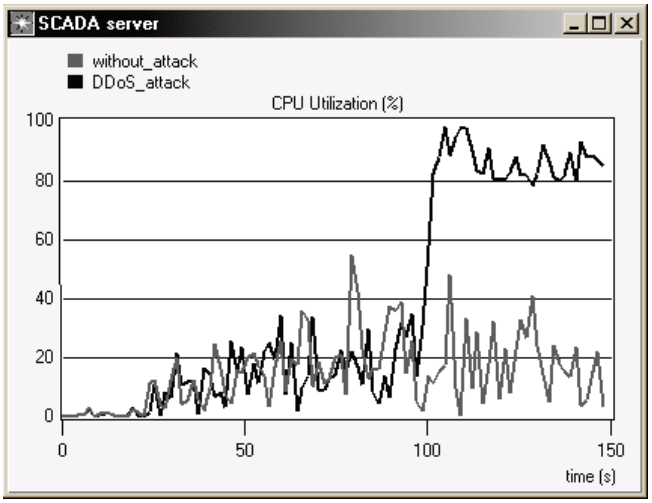

Fig. 5. CPU utilization at the victim node

From the obtain results, we can conclude that a high intensity of the incoming malicious traffic has caused blockage of the victim SCADA server resources. This can be seen in the utilization of processor time which is over 80%. At the moment the attack starts, due to congestion, packet dropping happens on the router interface towards the part of the network where the victim is located, so the level of dropped packets which belong to the traffic stream of the remote control operating service becomes increased and

comes to 3.6% in comparison to the total traffic in the highest priority queue. At the same time delay in processing the requests of legitimate traffic also increases.

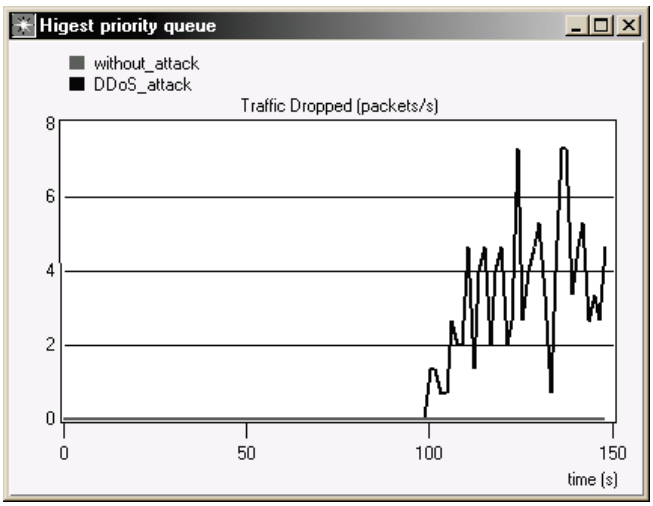

Fig. 6. Highest priority queue: Traffic dropped

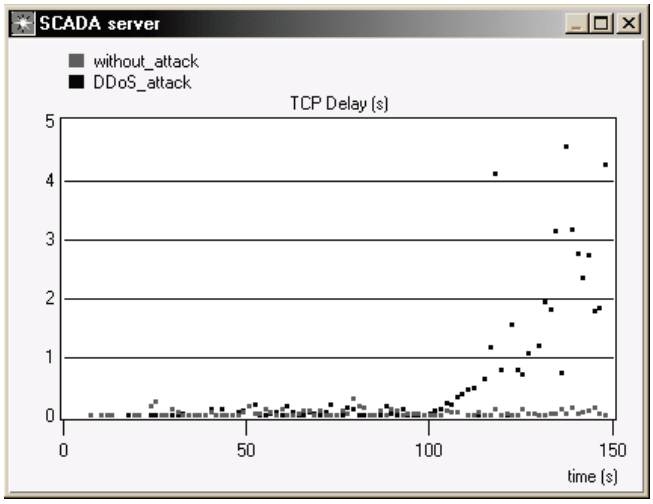

Fig. 7. TCP delay at the victim node

IV. Possible Solutions

At this time there is no comprehensive method of securing from the known forms of DDoS attacks. Possible security solutions can be listed as: (1) preventive, which are based on filtering with the aim of preventing the attacks; (2) reactive whose aim is to identify the attacker when the attack has already begun and (3) mechanisms following the attack which include the use of forensic analysis on the network [2]. We here give a brief overview of the main approaches in area of information privacy, detailed discussion can be found in [9], [10]. These approaches are of three types depending on their locality of deployment: victim-end, source-end and in–network approach. Detection approaches include statistical, soft-computing, clustering, knowledge-based and other data mining and machine learning methods.

Proper security and privacy have to become core requirements for any mechanism or application that is built. The education about privacy-enhancing technologies is an essential step in the roadmap towards security of digital world. Another important step is to make such technologies easy to deploy and use. Security of the data will require that these data be encrypted, both at rest and in transit, and that strong authentication mechanisms be used. This means that the user further needs support in managing their cryptographic keys and credentials. An application should be designed so that only the minimal amount of information gets revealed to each party that is necessary for the party to perform its task. Data minimization should be done at following layers: the network, the authentication and identities, and at last, application layer.

V. Conclusion

The evolution of modern SCADA systems architecture has led to identifying a number of security issues over the last decade. There are no safe mechanisms of defence from DDoS attacks, so this kind of attacks poses a serious threat to the infrastructure of advanced networks in power generation. The development of simulation models has provided the possibility of analysing the performances of remote control operating services in terms of DDoS attacks. The results of the simulation indicate to a degradation of performances and lack of services of the remote control operating services. In a broad sense, the safety of control systems is of great significance due to their irreplaceable role in the economy. This is why this is a current field of research where concrete improved solutions of SCADA systems security are anticipated.

References

[1] CIGRÉ Technical Brochures, “Integrated Service Networks for Utilities”, WGD2.07, 2004.

[2] A. Chakrabarti and G. Manimaran, “Internet Infrastructure Security: A Taxonomy”, *IEEE Network*, vol. 16, no.6, November/December 2002, pp. 13-21

[3] B. Zhu, A. Joseph, and S. Sastry, “Taxonomy of Cyber Attacks on SCADA Systems”, *Proceedings of CPSCom 2011: The 4th IEEE International Conference on Cyber, Physical and Social Computing*, Dalian, China, 2011.

[4] K. Barnes and B. Johnson, “Introduction to SCADA Protection and Vulnerabilities”, *Technical Report INEEL/EXT-04-01710, Idaho National Engineering and Environmental Laboratory*, Idaho Falls, Idaho, 2004.

[5] T. Tsiakis, "Information Security Expenditures: a Techno-Economic Analysis", *International Journal of Computer Science and Network Security*, 10. 4, April 2010, pp. 7-11.

[6] Technical Information Bulletin 04-1, “Supervisory Control and Data Acquisition (SCADA) Systems”, NCS TIB 04-1, Oct. 2004.

[7] R. L. Krutz, *Securing SCADA Systems*, Wiley, 2005.

[8] “OPNET IT Guru Academic Edition: A tool for networking education”, MSCIT Practicum Paper, Regis University [Online]. Available: http://www.opnet.com.

[9] T. Peng, C. Leckie and K. Ramamohanarao, “Survey of network-based defense mechanisms countering the DoS and DDoS problems”, *ACM Computing Surveys* 39, 1, Article 3, April 2007.

[10] J. Camenisch, “Information privacy?!”, Computer Networks, vol. 56, no. 18, Dec. 2012, pp. 3825-3833.