International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-2 Issue-15 June-2014

Development of an Attack-Resistant and Secure SCADA System using WSN, MANET, and Internet

N. Rajesh kumar[1], P.Mohanapriya[2], M.Kalaiselvi[3]

Abstract

Industrial Control Systems (ICS) are open to security attacks when they are integrated with IT systems and wireless technologies for enhanced processing and remote control. These Critical Infrastructures (CIs) are highly important as they provide service for an entire nation and causes serious danger even when interrupted for a while. Some of the common SCADA (Supervisory Control and Data Acquisition) systems involve energy and water distribution systems. In this paper, the energy distribution SCADA system comprising several substations is considered. A secure framework is proposed that combines the energy control system with Wireless Sensor Networks (WSNs), Mobile Ad hoc Networks (MANETs), and the Internet, providing anomaly prevention and status management. SCADA attacks occur at the state estimators of the power systems which are used to route power flows and detect faulty devices. These estimators are located in the SCADA control center which is a sensitive area and measurements must be transmitted over a secure communication channel. The attack-resistance of the SCADA system is enhanced by increasing the hardness and complexity of the attack problem. The Attack-Resistant and Secure (ARS) SCADA system is evaluated against existing techniques like NAMDIA (Network-Aware Mitigation of Data Integrity Attacks), Retrofit IDS (Intrusion Detection System), and CSBF (Critical State-Based Filtering) for enhancing the attack-resistance and security of SCADA systems. It is found that the performance of ARS SCADA system is good compared to the existing methods in terms of maximum normalized attack impact and latency.

Manuscript received June 17, 2014.

N. Rajesh kumar, Department of Electronics and Communication Engineering, Pollachi Institute of Engineering and Technology, Pollachi, Tamil Nadu, India.

P. Mohanapriya, Department of Information Technology, Dr. Mahalingam College of Engineering & Technology, Pollachi, Tamil Nadu, India.

M. Kalaiselvi, Department of Electronics and Communication Engineering, Pollachi Institute of Engineering and Technology,Pollachi, Tamil Nadu ,India.

Keywords

IDS (Intrusion Detection System), Mobile Ad hoc Networks (MANETs), SCADA (Supervisory Control and Data Acquisition), State Estimator, and Wireless Sensor Networks (WSNs).

1. Introduction

Supervisory Control and Data Acquisition (SCADA) systems are used in various Industrial Control Systems (ICS) in fields like water and energy distribution. When these control systems are integrated with the emerging wireless technologies and Internet, they are prone to various security challenges and attacks. The SCADA system under consideration is an energy distribution system. An architecture comprising Wireless Sensor Networks (WSNs), Internet, and Mobile Ad hoc Networks (MANETs) is applied to enhance the energy control processes.

Low-powered sensor nodes (SNs) of the WSNs are used to sense the information, process them, and transmit them to a powerful base station (BS). The BS routes the information to the SCADA center or nearby operators. The functionality of SNs extends beyond the conventional information retrieval by providing alerting schemes and triggering alarms under intrusive conditions. Another important property is the self-configurability and self-healing capability under of nodal failures or attacks. The communication standards of the WSN enable the coexistence with other communication networks like MANET.

MANETs serve as an alternate communication between remote substations and operators. Mobility is offered to the operators close to the substation who can monitor the sensed information without going through the SCADA center. This architecture is self-organizing which can be easily established without any other infrastructure while permitting operators to access the solutions to critical alarms. It facilitates a quicker system reconfiguration in case of emergency events.

Web-based SCADA system enables the entire system to enhance the control processes individually irrespective of their geographic locations. So

authenticated operators can remotely monitor/access a substation. The use of open web protocols decreases the installation cost of Hardware/Software (HW/SW) sections.
The remaining part of the paper is organized as follows: Section II involves the works related to probable solutions for security issues in SCADA. Section III involves the description of the attack-resistant and secure (ARS) SCADA system. Section IV involves the performance analysis of the ARS SCADA system and existing techniques based on NAMDIA (Network-Aware Mitigation of Data Integrity Attacks), Retrofit IDS (Intrusion Detection System), and CSBF (Critical State-Based Filtering). The paper is concluded in Section V.

2. Related Work

This section deals with various methods for enhancing the security and attack resistance of SCADA system. Cybersecurity in SCADA systems is an important issue, as they control the critical infrastructures (CI) of a nation[1]. By evaluating the attack vectors and high-ranking vulnerabilities the success of the attack can be significantly reduced. The security of SCADA networks combined with IP networks is efficiently managed by proper network traffic analysis and identification of network usage patterns [2], [3], [4]. The network security analysis by minimum cut relaxation method is used for the strategic allocation of protection devices in SCADA networks [5]. The security of SCADA systems is realized in water distribution systems[6], [7] and smart grids [8], [9].

The improvement of resilience and robustness of CIs relative to cyber-attacks is studied in [10]. Some of the issues in SCADA systems are protection of the information and data flow, early detection, isolation, and elimination of cyber hazards. The automatic and reconfigurable SCADA systems are not fully secure because of the possible human interventions. So, the SCADA system is designed to handle the human interventions via offline tools. In [11], customized normalcy profiles and behavioral modeling was used for protection against cyber-attacks. Behavioral modeling on higher semantic levels enhances the efficiency of the anomaly detection.

Alzaid, et al., proposed secure key management schemes employed in WSNs for Process Control Systems (PCS)/SCADA systems for enhancing the security and avoiding sandwich attacks[12], [13]. PCS/SCADA architecture enables convenient use of cryptographic mechanisms. This method is resistant to node capture attacks via forward and backward authentication schemes. Hadžiosmanović, et al., proposed a log mining method for process monitoring in SCADA systems [14]. It detects the process-related threats when an attacker acts as a legitimate user and executes the system operations. A semi-automated scheme of log processing is used to avoid these kinds of attacks.

Vukovic, et al., proposed a protection technique against stealth attack in the state estimators of SCADA power systems [15], [16]. A state estimator is used to compute the optimal power flow and detect error-prone devices. Different application layer and network layer security strategies are used to reduce the vulnerability of the state estimator. The resilience of critical SCADA system is enhanced using Peer-to-Peer (P2P) overlays [17]. The integration of IT systems with SCADA systems possesses new threats as it becomes more accessible. These threats result in decreased system availability, longer processing time, and risks to public safety. P2P networks involve two inherent resilience schemes namely, data replication and path redundancy.

An IDS is developed upon the assumption of fair and normal traffic in SCADA system [18]. The linking of the network flows enhances the accuracy of the anomalous traffic information, which aids in intrusion detection. *Morris* and *Pavurapu* used a multi-layer and secure retrofit network data logger for statistics based and signature based intrusion detection systems in electricity substations [19]. The electricity (transmission and distribution) substations contain critical modules such as Remote Terminal Units (RTUs), Phasor Measurement Units (PMUs), Intelligent Electronic Devices (IEDs), Phasor Data Concentrators (PDC), and relays. These CI assets are secured using firewalls. The retrofit data logger is applied for MODBUS and DNP3 (Distributed Network Protocol) based SCADA systems to enable the control systems to be updated. The network log transactions are updated with substation based network intrusion detection. The data logger acts as an embedded bump-in-the-wire device for authentication and storage of network traffic.

Fovino, et al., proposed a critical state-based filtering scheme for securing the SCADA network protocols [20]. The filter systems are based on the state analysis of the monitored system and firewalls for

MODBUS and DNP3.*Mander*, *et al*., enhanced the data object security of SCADA power systems employing DNP3 [21]. A rule-based security is utilized for power distribution devices based on DNP3. It involves data objects and DNP3 application layer function codes to evaluate the data access authorization for users. Datasets are used to reduce the security complexity by rule reduction, which enhance the security of process constrained devices.

3. Attack-Resistant and Secure SCADA System

The ARS SCADA system improves the security of the system by an integrated approach of WSN, MANET, and the Internet, while the attack-resistance is guaranteed by increasing the hardness and complexity of the attack problem.

A. Combining WSN, MANET, Internet for a secure SCADA system

The integrated framework of WSN, MANET, and Internet with SCADA system has the ability to detect anomalous events and faults in the system. The SNs are deployed in the entire system for data acquisition pertaining to energy generation, distribution, and usage. The details are sent back to the SCADA center to control the energy generation and distribution. The integration of WSN and MANET enables the operators to detect a malfunction by sensors and manage the data streams. MANETs permits the establishment of collaborative communications with other operators for quicker response during emergency situations.

The remote WSN can be managed by a SCADA center or distant operators, which manages the real-time queries, control processes, and anomalous behaviors. The sensor nodes of the WSN use the Internet to generate failure/threat alerts in order to avoid situations that may disturb the normal services. The Internet maximizes the collaboration capabilities by offering management and reliability of services.
The WSN and SCADA center are connected via a BS, whose use will depend on both requirements of network topology and the communication standards like Zigbee PRO, WirelessHART (Highway Addressable Remote Transducer Protocol), and ISA.100.11a. Connectivity models such as, Front-End proxy solution, Gateway solution, and TCP/IP solution, links the WSN with the Internet. The most appropriate connectivity model can be determined according to their complexity and effects upon the system. The Front-End solution is the most suitable one as the WSN is completely independent from the Internet, and the system can issue control commands and access the data streams. This solution will concentrate all the computational overhead in a group of BSs, whose function will be to break down and store the information. The BSs interpret and translate the SCADA control commands to a protocol which it can understand.

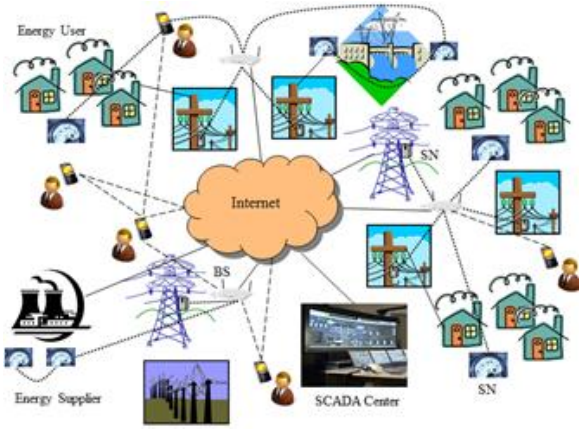

Fig. 1. Combining WSNs, MANETs, and Internet for a secure SCADA system.

Fig. 1 shows an overview of the integrated approach of WSNs, MANETs, and the Internet with the SCADA system. Security is important in this architecture, as data streams have to be communicated with various types of networks and processed on various devices with dissimilar configurations. The intrusion of attackers can be avoided by designing cryptographic schemes and optimizing the block size of cipher text relative to the message size. This will reduce the communication overhead, network traffic, packet loss, save the constrained bandwidth, energy consumption, and thereby prolong the network lifetime.

The communication between the different entities of the SCADA system is highlighted in Fig. 2. The system should be reliable to fulfill the CI protection standards. This necessitates that the alarms and sensing data streams should reach the SCADA control center in a secure, reliable, and timely manner. The backup communication streams should be readily available in case of security attacks. The number of BSs can be increased to improve the availability of alternate paths and mitigate the attacks.

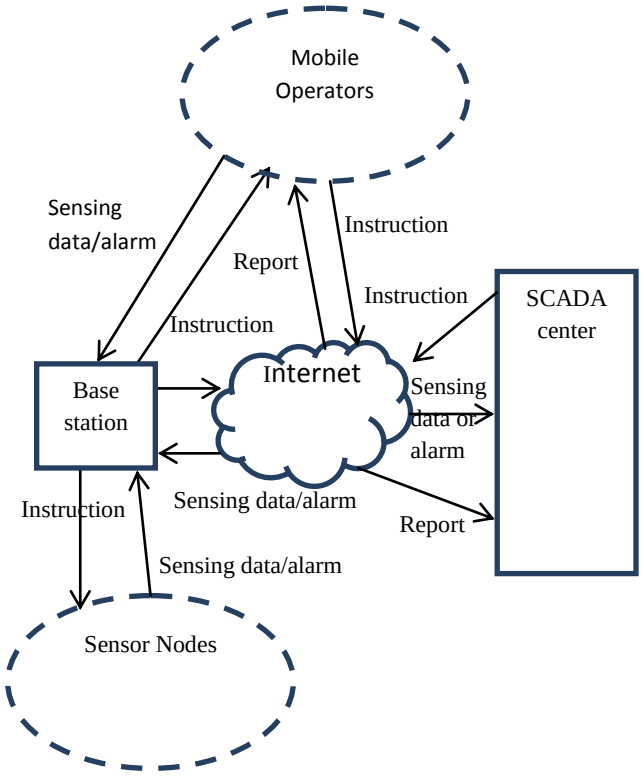

Fig. 2. Communication between different elements of SCADA system.

Increasing the attack-resistance of SCADA system

The SCADA power system consists of $i + 1$ buses, and there are j meters that display power flow measurements x to the state estimator via communication channels. An attacker is capable of alter from x into $x_y := x + y$, either by physical tampering or unauthorized access to some communication channels.y is the attack vector added to the original measurement x. The attacker's goal is to fool the Energy Management System (EMS) and the operator that a specific power flow measurement is $x_{z,y} = x_z + y_z$ and not x_z, for some z and fixed scalar y_z. Stealth attacks occur when the Bad Data Detection (BDD) system in the SCADA control center is not triggered. The corruption of the measurement x_y into $x_z + y_z$ will generally invoke a bad-data alarm.

A set of measurements $\{1,\ldots, j\}$ is partitioned into a set of blocks $J = \{J_1,\ldots, J_{|J|}\}$ to determine the cost of the operator and the attacker. All measurements belonging to the block J_a of the a^{th} bus can be protected at unit cost. The matrix of the order $|J|$ x j is denoted by U, whose element $U_{az} = 1$ if $z \in J_a$, and $U_{az} = 0$ otherwise. The cost of an attack y for the attacker is equivalent to the number of non-zero elements in the vector $U|y|$ denoted by $\|U|y|\|_0$. $|y|$ gives the vector form of the magnitudes of entities in y. A subset of the partition authenticated by the operator is denoted as $V \subseteq 2^J$.

An attacker can apply any undetectable attack vector y, $y_z \neq 0$ to attack measurement z. The attacker would be focused on determining an attack vector y, $y_z \neq 0$ with minimum cost, under the condition that the attacker cannot square off any protected measurement $z \in V$. The attacker has to solve the following problem to determine a minimal stealth attack on z.

$$\alpha_z := \min_v \|U|Mv|\|_0, \quad (1)$$

$$\text{s.t.} \quad \sum_b M_{zb} v_b = 1, (Mv)_a = 0 \; \forall \; a \in V \quad (2)$$

M is the Jacobian matrix determined at unknown bus phase angles from x and v is an arbitrary vector. In (1), the corruptions that do not compromise protected measurements and trigger bad-data alarms are optimized. The minimal stealth attack problem is generally hard to solve and non-convex. The attacks are determined with a minimal cost by an iterative path augmentation algorithm.

4. Performance Analysis

ARS SCADA system is evaluated against existing techniques for enhancing the attack-resistance and security of SCADA systems. The existing methods include NAMDIA [16], Retrofit IDS [19], and CSBF [20]. The following parameters are analyzed for the performance evaluation of ARS SCADA:

A. Maximum normalized attack impact

The substation attack impact is a metric which relates the count on which an attacker gain access into a substation and perform a stealth attack. Lesser is the attack impact, higher would be the protection of the SCADA system. The maximum normalized attack impact is evaluated with respect to four variable counts namely, single-path routes altered, multi-path routes, non-tamper-proof authenticated RTUs, and tamper-proof authenticated RTUs.

1) Number of single-path routes altered

The maximum normalized attack impact versus the number of single-path routes altered is analysed between NAMDIA and ARS SCADA in Fig. 3.

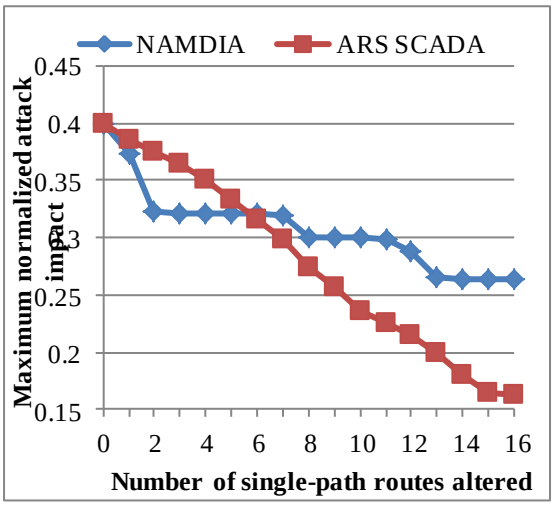

Fig. 3. Maximum normalized attack impact vs. the number of single-path routes altered.

2) Number of multi-path routes

The maximum normalized attack impact versus the number of multi-path routes is analyzed between NAMDIA and ARS SCADA in Fig. 4. The attack impacts are evaluated for different attack costs (C1 and C2).

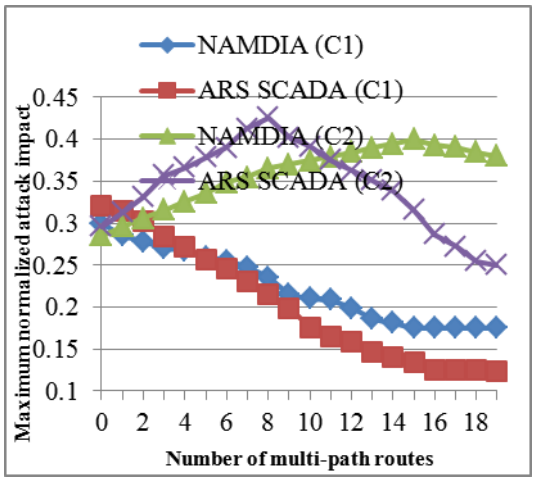

Fig. 4. Maximum normalized attack impact vs. the number of multi-path routes for attack cost 1 and cost 2.

3) Number of non-tamper-proof authenticated RTUs

The maximum normalized attack impact versus the number of non-tamper-proof authenticated RTUs is analysed between NAMDIA and ARS SCADA in Fig. 5.The attack impacts are evaluated for different attack costs (C1 and C2).

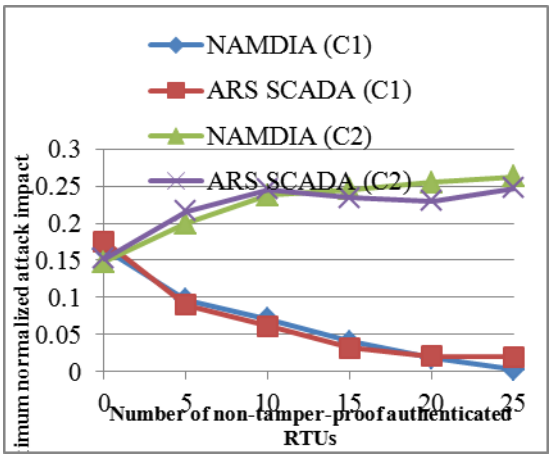

Fig. 5. Maximum normalized attack impact vs. the number of non-tamper-proof authenticated RTUs for attack cost 1 and cost 2.

4) Number of tamper-proof authenticated RTUs

The maximum normalized attack impact versus the number of tamper-proof authenticated RTUsis analyzed between NAMDIA and ARS SCADA in Fig. 6.The attack impacts are evaluated for different attack costs (C1 and C2).

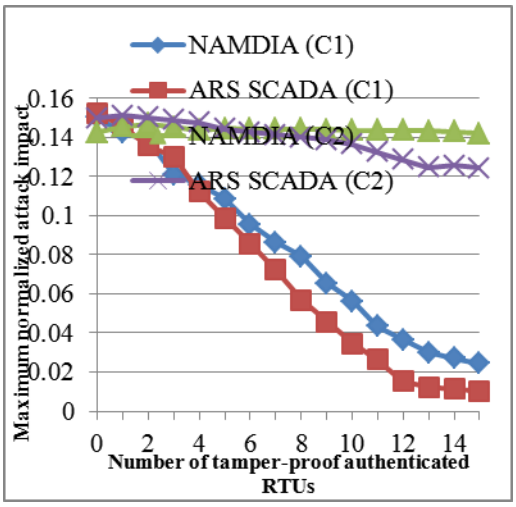

Fig. 6. Maximum normalized attack impact vs. the number of tamper-proof authenticated RTUs for attack cost 1 and cost 2.

B. Latency

Latency is evaluated with respect to two parameters namely, Link layer Protocol Data Unit (LPDU) length and data rate.

1) LPDU length

Latency versus the LPDU length is analyzed between Retrofit IDS and ARS SCADA is analyzed in Fig. 7.

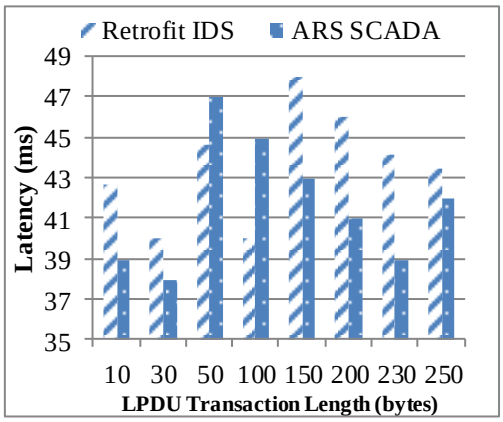

Fig. 7. Latency vs. LPDU length.

2) Data rate

Latency versus the data rate is analyzed between CSBF and ARS SCADA is analyzed in Fig. 8. This gives the communication latency in the system.

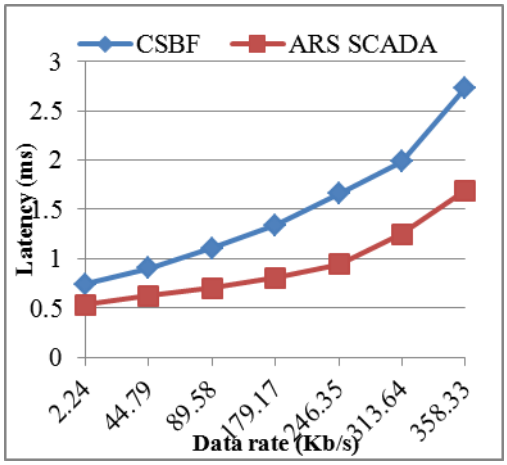

Fig. 8. Communication latency.

5. Conclusion

Critical Infrastructures (CIs) such as SCADA systems are important owing to its huge nationwide coverage area. A failure or attack to these systems results in drastic changes in the service distribution. These effects may also be serious or cascading resulting in disruption of other essential services. These control systems when combined with web-based applications become insecure and less bounded. In this paper, Low powered Sensor Nodes (SNs) of a Wireless Sensor Network (WSN), Mobile Ad hoc Networks (MANETs), and Internet are chosen to aid mobile operators and receive real-time alerts. This framework provides management, mobility, collaboration, detection, alert, and response. The Attack-Resistant and Secure (ARS) SCADA system is evaluated against existing techniques like NAMDIA (Network-Aware Mitigation of Data Integrity Attacks), Retrofit IDS (Intrusion Detection System), and CSBF (Critical State-Based Filtering) for enhancing the attack-resistance and security of SCADA systems. It is found that the performance of ARS SCADA system is good compared to the existing methods in terms of maximum normalized attack impact and latency.

References

[1] J. Hull, et al., "Staying in Control: Cybersecurity and the Modern Electric Grid," Power and Energy Magazine, IEEE, 2012, vol. 10, no. 1, pp. 41-48.

[2] A. N. Mahmood, et al., "Network Traffic Analysis and SCADA Security," in Handbook of Information and Communication Security, P. Stavroulakis and M. Stamp, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 383-405.

[3] H. Kim, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," International Journal of Distributed Sensor Networks, 2012, vol. 2012,pp. 1-10.

[4] C. Alcaraz, et al., "Security Aspects of SCADA and DCS Environments," in Critical Infrastructure Protection. vol. 7130, J. Lopez, R. Setola, and S. Wolthusen, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 120-149.

[5] S. Kin Cheong, et al., "Electric power network security analysis via minimum cut relaxation," in Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on, 2011, pp. 4054-4059.

[6] S. Amin, et al., "Cyber Security of Water SCADA Systems-Part I: Analysis and Experimentation of Stealthy Deception Attacks," Control Systems Technology, IEEE Transactions on, 2012,vol. PP,no. 99, pp. 1-1.

[7] S. Amin, et al., "Cyber Security of Water SCADA Systems-Part II: Attack Detection Using Enhanced Hydrodynamic Models," Control

Systems Technology, IEEE Transactions on, 2012,vol. PP,no. 99, pp. 1-1.
[8] G. N. Ericsson, "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure," Power Delivery, IEEE Transactions on, 2010, vol. 25, no. 3, pp. 1501-1507.
[9] A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks," Smart Grid, IEEE Transactions on, 2010, vol. 1, no. 1, pp. 99-107.
[10] A. Amantini, et al., "The human role in tools for improving robustness and resilience of critical infrastructures," Cognition, Technology & Work, 2012, vol. 14, no. 2, pp. 143-155.
[11] A. Dolgikh, et al., "Using Behavioral Modeling and Customized Normalcy Profiles as Protection against Targeted Cyber-Attacks," in Computer Network Security. vol. 7531, I. Kotenko and V. Skormin, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 191-202.
[12] H. Alzaid, et al., "A Forward and Backward Secure Key Management in Wireless Sensor Networks for PCS/SCADA," in Sensor Systems and Software. vol. 24, S. Hailes, S. Sicari, and G. Roussos, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 66-82.
[13] H. Alzaid, et al., "Mitigating Sandwich Attacks Against a Secure Key Management Scheme in Wireless Sensor Networks for PCS/SCADA," in Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, 2010, pp. 859-865.
[14] D. Hadžiosmanović, et al., "A log mining approach for process monitoring in SCADA," International Journal of Information Security, 2012, vol. 11,no. 4, pp. 231-251.
[15] O. Vukovic, et al., "Network-layer protection schemes against stealth attacks on state estimators in power systems," in Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, 2011, pp. 184-189.
[16] O. Vukovic, et al., "Network-Aware Mitigation of Data Integrity Attacks on Power System State Estimation," Selected Areas in Communications, IEEE Journal on, 2012, vol. 30, no. 6, pp. 1108-1118.
[17] D. Germanus, et al., "Increasing the Resilience of Critical SCADA Systems Using Peer-to-Peer Overlays," in Architecting Critical Systems. vol. 6150, H. Giese, Ed., ed: Springer Berlin Heidelberg, 2010, pp. 161-178.
[18] R. Barbosa and A. Pras, "Intrusion Detection in SCADA Networks," in Mechanisms for Autonomous Management of Networks and Services. vol. 6155, B. Stiller and F. Turck, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 163-166.
[19] T. Morris and K. Pavurapu, "A retrofit network transaction data logger and intrusion detection system for transmission and distribution substations," in Power and Energy (PECon), 2010 IEEE International Conference on, 2010, pp. 958-963.
[20] I. N. Fovino, et al., "Critical State-Based Filtering System for Securing SCADA Network Protocols," Industrial Electronics, IEEE Transactions on, 2012, vol. 59, no. 10, pp. 3943-3950.
[21] T. Mander, et al., "Power system DNP3 data object security using data sets," Computers & Security, 2010,vol. 29,no. 4, pp. 487-500.

N. Rajeshkumar was born in India, Tamilnadu on 5th April 1980.He received his Bachelors Degree from Periyar University Salem and his Master Degree in Anna University, and Chennai.Currently he is working as an Assistant Professor in Pollachi Institute of Engineering and Technology with nearly 8 Years of Teaching Experience and pursuing his research in the area of Network Security. He is Interested in Digital Electronics, Network Security, Cyber Security & Communication Systems. He is Lifetime Member of ISTE and an active member of IEEE.He is Professional Member of International Association of Electronics and computer Engineering. He was certified by Oracle Corporation as Oracle certified professional and administrator.

Mrs. P. Mohanapriya was born in India; Tamilnadu on 19th September 1987.She received her Bachelor Degree in Computer Science under Anna University Chennai and did her Master Degree in Software Engineering at Anna University of Technology Coimbatore. Currently she is working as an Assistant Professor in Dr.Mahalingam College of Engineering & Technology. She is having 4 years of academic Experince.Her interests included Database Management, Software Engineering, Network security & Data Structures. She is Lifetime Member of ISTE.

M. Kalaselvi was born in India, Tamilnadu on 9th March 1986. She received her B.E. under Anna University Chennai and Master Degree from Anna university of Technology Coimbatore. Currently she is working as Assistant Professor in Pollachi Institute of Engineering and Technology. She is having 5 years of Teaching Experience. She is Interested in VLSI Design, LIC, Digital Signal Processing and Networks.