AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

A Secure Framework for SCADA Trust System in Critical Infrastructures

[1]N. Rajesh kumar and [2]Dr. P. Jaganathan

[1]*Assistant Professor, Department of ECE, Pollachi Institute of Engineering and Technology, Pollachi-642205, Tamil Nadu, India,*
[2]*Professor, Department of MCA, PSNA College of Engineering and Technology, Dindugul-624622, Tamil Nadu, India,*

ARTICLE INFO

Article history:
Received 19 August 2014
Received in revised form
19 September 2014
Accepted 29 November 2014
Available online 15 December 2014

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

ABSTRACT

SCADA [Supervisory control and data acquisition] is a system operating with coded signals over communication channels provides control for remote equipments. It is a type of Industrial Control System [ICS] to monitor and process controlling that exists in the physical world. These Bottleneck Infrastructures [BIs] are open to security attacks when they are combined with IT systems and wireless technologies for process enhancing and controlled remotedly. Nationally, most of the energy and water distributed systems can be operated by using SCADA. Our research is focused on prevention by behavioral and operational management by using Wireless sensor nexus, Blower Ad hoc web and the cyberspace. Generally, attack happens at the state estimators of a system which are used to route power flows and identify erroneous devices. State estimators are placed in a sensitive area of SCADA control center to transmit the data's in a safe communication channel which is ensured by expand the hardness and complexity of the attack problem. Our proposed ARS [Attack Resistance Secure] SCADA system is analyzed against the available techniques like NAMDIA [Network-Aware Mitigation of Data Integrity Attacks], Retrofit IDS [Intrusion Detection System] and CSBF [Critical State Based Filtering] for improving the attack resistance and security of SCADA system. By evaluating maximum normalized attack impact and latency in the existing system, the ARS SCADA system is found to be good in terms of its performance.

To Cite This Article: N. Rajesh kumar and Dr. P. Jaganathan, A Secure Framework for SCADA Trust System in Critical Infrastructures. ***Aust. J. Basic & Appl. Sci.,*** *8(18): 143-150, 2014*

INTRODUCTION

SCADA used in several ICS in domains like water and energy partitioning. When these supremacy systems are unified with the emanate wireless technologies and cyberspace, they are inclining to various pledging challenges and encroachment. The SCADA system under deliberation is an energy disseminating system. An architecture comprising wireless sensor networks, the cyberspace and blower ad-hoc web is applied to elevate the energy control processes.

WSN of spatially distributed self governing sensors to scrutinize physical and environmental conditions. Base station seize the sensed information from low powered Sensor Node[SNs] of the WSN. The base station routes the statistics to the entire operators of SCADA.SNs indulge the alerting schemes and alarms under obtrusive conditions. Additionally, vital property is the self configurability and remedial ability related to failures.WSN empowers the synchronicity with alternative communication networks.

The proxy communication between remote substations and operators is attained by mobile ad-hoc network further labeled as blower ad-hoc web. The operators nearby the substations can supervise the sensed information without going through the SCADA center is obtained by portability offered to the operators. The operators are authorized to approach the clarification to critical alarms. This architecture is self standardize which can be efficiently entrenched without other infrastructure. In case of emergency phenomenon, this architecture expedites an energetic system reconfiguration.

Irrespective to the geographic locations web based SCADA systems facilitates the integral system to escalate the control process distinctively. So, authenticated operators can incidentally ingress a substation. The implementation tariff of hardware and software section is diminished by the use of open web protocol.

The remaining of the paper is catalogued as: In the foremost category, security controversy in SCADA and its probable elucidation is concerned. Second category suggests the summarization of Attack-Resistant and Secure [ARS] SCADA system. The tertiary category implies the pursuance analysis of the ARS SCADA system

Corresponding Author: N. Rajesh kumar Assistant Professor, Department of ECE, Pollachi Institute of Engineering and Technolog, Pollachi-642205, Tamil Nadu, India.
Tel: +919843844844 E-mail: rajeshkumar.n1@gmail.com

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 143-150

and current techniques positioned 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 uppermost category.

II. Related Work:

This category is arranged with numerous methods for exaggerating the security and attack resistance of SCADA systems. The critical infrastructures of a nation are controlled by cyber security in the SCADA system which is a peculiar controversy (Hull, 2012). The success of the attack can be significantly declined by estimating the attack vectors and high ranking vulnerabilities. By analyzing proper network traffic and identification of network usage pattern is efficiently influenced by combining SCADA with IP (Mahmood, 2010; Kim, 2012; Alcaraz, 2012). The network surveillance analyze is used for strategic appropriation of protection device in SCADA network by minimum cut relaxation method (Kin Cheong, 2011). In water distribution system (Amin, 2012; Amin, 2012) and smart grids (Ericsson, 2010; Metke and Ekl, 2010) the security of SCADA system is accomplished.

The resilience and robustness of CIs reliant to cyber attack is enhanced in (Amantini, 2012). The preservation of information and data flow, early detection, isolation and cutoff cyber endangerment. Because of possible human interventions the automatic and reconfigurable SCADA systems are not fully secured. So the SCADA system is delineated to handle the human interventions via offline tools. Behavioral modeling on higher linguistic levels escalates the effectualness of the anomaly detection is personalized (Dolgikh, 2012).

The secure key management schemes hired in WSN for process control systems/SCADA system for enlarging the security and obviate sandwich attacks (Alzaid, 2010; Alzaid, 2010). Cryptographic mechanisms is contrary to node capture attacks via forward and backward authentication proposals.PCS/SCADA architecture accredit cryptographic mechanism (Hadžiosmanović, 2012). A semi automated scheme of log processing is used to avoid the process related threats when an attack act as an legitimate user and executes the system operations.

The protection approach against stealth attack in the state estimators of SCADA systems intended (Vukovic, 2011; Vukovic, 2012). To enumerate optimal power flow and detect error prone device state estimators are used. The flexibility of critical SCADA system is intensified using Peer To Peer[P2P] overlays (Germanus, 2010). P-P network implies two essential resilience proposal namely data replication and path redundancy. New threats are possessed when SCADA systems are assimilated with IT systems.

In consequent to hypothesis of fair and normal traffic in SCADA system an IDS is developed. In coupling of the network flows heightens the accuracy of the heteroclite, traffic information which aids in intrusion detection (Barbosa and Pras, 2010). In electricity substations, multilayer, secure retrofit network data logger is used for statistics based and signature based intrusion system (Morris and Pavurapu, 2010). The critical modules such as Remote Terminal Units[RTUs], Phasor Measurement Units[PMUs], Intelligent Electronic Devices[IEDs], Phasor Data Concentrators[PDCs] and relays is composed in electrical substations. To accredit the control systems to be updated, the retrofit data logger is applied for MODBUS and DNP3 [Distributive Network Protocol] based SCADA systems. For authentication and storage of network traffic, the data logger act as an embedded bump in the wire device. The network log transactions are updated with substation based network intrusion detection.

For procuring SCADA network protocols critical state based filtering scheme is proffered (Fovino, 2012). On the state analysis of the monitored system and firewalls for MODBUS and DNP3, the filter systems are established. The data object security of SCADA power systems utilizing DNP3 is magnified in (Mander, 2010). A rule based security is employed for power distribution devices based on DNP3.It implicates data, object and DNP3 application layer function codes to estimate the data approach endorsement for users. To escalate the preservation of process constrained devices, data sets are used to weaken the security complication by rule devaluation.

III.Attack-Resistant and Secure SCADA System:

The ARS SCADA system boost the security of the system by an integrated approach of WSN,MANET and the cyberspace, while the attack resistance is insured by rising the hardness and entanglement of attack obstacle.

A) Merging WSN, MANET, Internet secure SCADA systems:

The capability to recognize the anomalous events and error in the system, the WSN, MANET, Internet with SCADA are unified. For data acquisition pertaining to energy generation, distribution and usage, the SNs are deployed in the entire system. The particular details are directed back to the SCADA center to control the energy generation and distribution. The unified WSN and MANET permit the operators to identify the malfunctions by sensors and administrate the data streams. During emergency situation MANET allows the formulation of collaborative communication with other operators for energetic response.

The real time skepticisms, control processes and heteroclite attitude are managed by remote WSN, which is handled by SCADA center or distant operators. In order to avert the situations that may interrupt the normal

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 143-150

services, the sensor nodes of WSN use the cyberspace to provoke failure/threat alerts. By offering management and reliability of services, the cyberspace overestimates the collaboration capabilities.

The WSN and SCADA centers depends on both specification of network topology and the communication standards like ZigbeePRO,WirelessHART[Highway Addressable Remote Transducer Protocol] and ISA.100.11a and connected via a BS. The WSN and cyberspace are interlinked by connectivity models such as frontend proxy solution, gateway solution and TCP/IP solution. According to the complexity and effects upon the system the appropriate connectivity model can be determined. The front end solution is the most sufficient one as the WSN is ultimately independent from the internet and the system can issue control commands and approaches the data streams. This approach will focus all the computational overhead in a group of BSs, its function will be to break down and store the essential information. The BSs interpret and decipher the SCADA control commands to a protocol which it can accept.

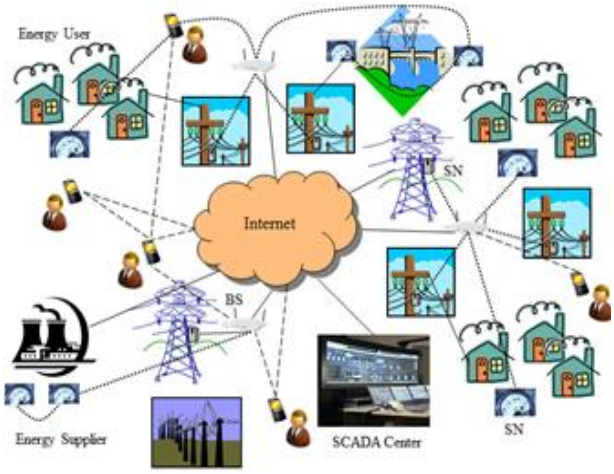

Fig. 1: Merging WSN, MANET, INTERNET secure SCADA systems.

Figure1 displays the overview of the unified path of WSNs, MANETs and the cyberspace with the SCADA system. Preservation is crucial in this architecture, as data streams have to be disclosed with numerous types of networks and processed on different devices with dissimilar structures. By designing cryptographic schemes and optimizing the block capacity of cipher text relative to the message capacity, the invasion of the attackers can be fend offed. This will curtail the communication overhead, network traffic, packet loss, save the constrained bandwidth, energy consumption and thereby perpetuate the network lifetime.

The communication between the several entities of the SCADA system is highlighted in figure2.The system should be predictable to fulfill the BI protection standards. This necessitates that the alarms and scrutinizing data streams should reach the SCADA control center in a secure, reliable and timely aspect. In case of security attacks, the backup communication streams should be readily feasible. To improve the availability of the equivalent paths and mitigate the attacks, number of BSs should be increased.

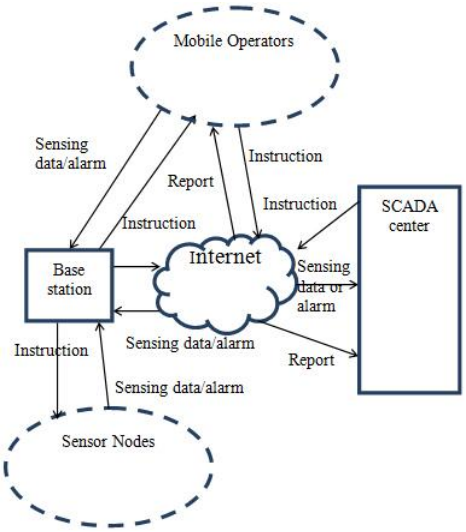

Fig. 2: Communication between the several entities of the SCADA system.

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 143-150

B) Increasing the attack-resistance of SCADA systems:

The SCADA power system subsists of $i + 1$ buses, and j meters which display power flow measurements x to the state estimator via communication channels. An attacker is attacker is competent of amend from x into $x_y := x + y$, either by substantial tampering or illegitimate approach to some communication channels. The original measurement x is added with the attack vector y. The attacker's intension is to fool the Energy Management System [EMS] and the operator that a precise power flow measurement is $x_{z,y} = x_z + y_z$ and not x_z, for some z and fixed scalar y_z. When the Bad Data Detection [BDD] system in the SCADA control center is not triggered stealth attack occurs. It will invoke a bad data alarm when the measurement x_y into $x_z + y_z$ is corrupted.

To regulate the cost of operator and the attacker a set of measurement $\{1,\ldots, j\}$ is portioned into a set of block $J = \{J_1,\ldots, J_{|J|}\}$. The measurement associated to block J_a of the a^{th} bus can be protected at unit cost. The order of the matrix $|J|$ x j is denoted by U, whose element $U_{az} = 1$ if $z \in J_a$, and $U_{az} = 0$ otherwise. The number of non-zero elements in the vector $U|y|$ denoted by $\|U|y|\|_0$ is equivalent to cost of an attack y for the attacker. $|y|$ 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, $y_z \neq 0$. The attacker cannot square off any protected measurement $z \in V$ and the attacker would be focused on determining vector y, $y_z \neq 0$ with minimum cost. To determine a minimal stealth attack on z.

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

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

x and v is an arbitrary vector unknown bus phase angles which is determined by Jacobean matrix M. The corruptions that do not compromise protected measurements and trigger bad data alarms are improved in (1). The minimal stealth attack problem is normally hard to solve and non-convex. By an iterative path augmentation algorithm the attacks are resolute with minimal cost.

IV. Performance Analysis:

To embellish the attack-resistance and security of SCADA system, ARS SCADA system is appraised against actual techniques include NAMDIA [16], Retrofit IDS [19], and CSBF [20]. The performance analyses of ARS SCADA system are as follows:

A. Supreme Standardized attack impact:

Impact of an attack in substation is a metric which reveal the count on which an attacker gain connects into a substation and a stealth attack is performed. The security of SCADA system is superior, while the attack impact is diminished.

The attack impact is criticized with respect to four important measures are specially mentioned as, modified single-path routes, flight-path routes, non-tamper-proof substantiate RTUs, and tamper proof substantiate RTUs.

1) Number of Modified single-path routes:

The normalized attack impact versus number of modified single-path routes is scrutinized between MAMDIA and ARS SCADA.

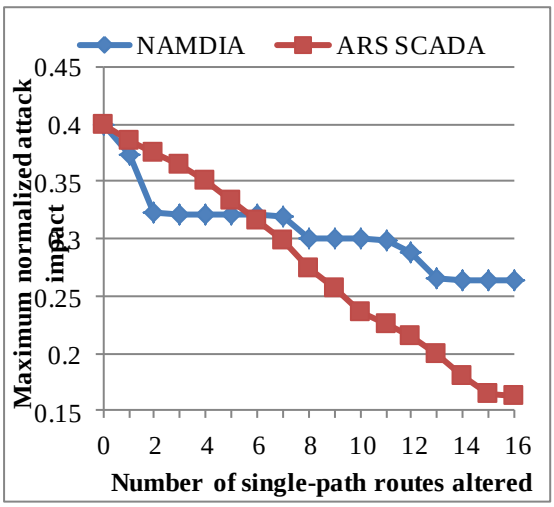

Fig. 3: Normalized impacts versus number of modified single-path routes.

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 143-150

2) Number of flight-path routes:

The maximum normalized attack impact versus the number of flight-path routes analyzed between NAMDIA and ARS for distinct attack cost (c1 and c2).

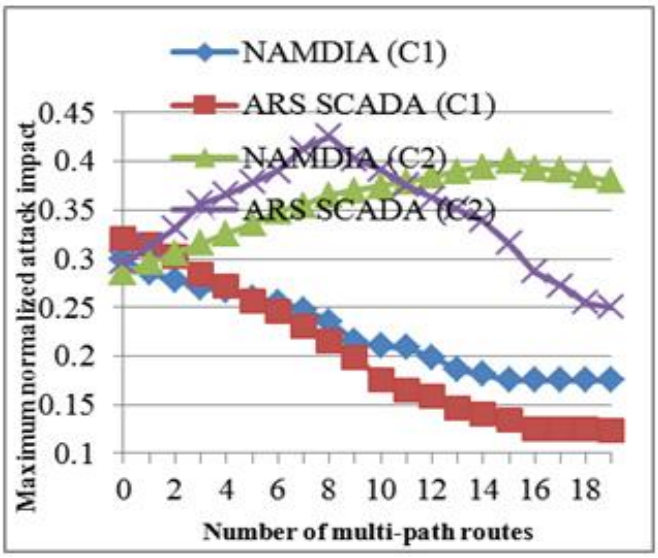

Fig. 4: Maximum normalized attack impact versus the number of flight-path routes for cost 1 and cost2.

3) Number of non-tamper-proof substantiate RTUs:

The maximum normalized attack impact versus the number of non-tamper-proof substantiate RTUs is figure out between NAMDIA and ARS SCADA. Attack impacts are evaluated at different costs (C1 and C2).

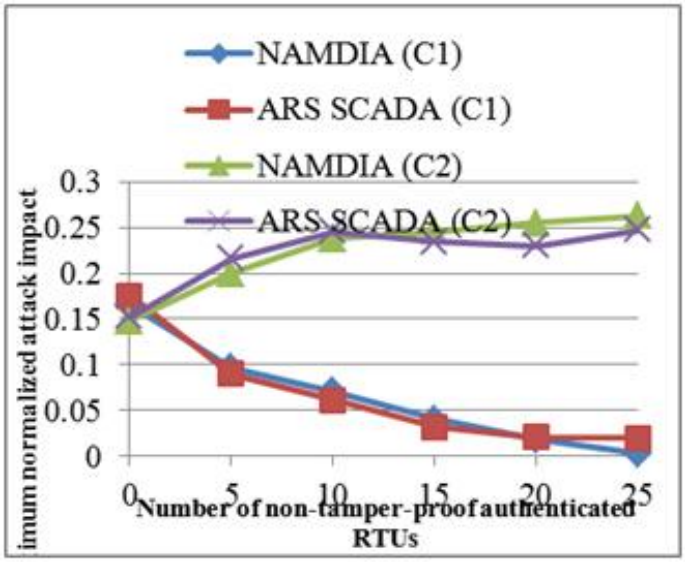

Fig. 5: Maximum normalized attack impacts versus the number of non-tamper proof substantiate RTUs for cost 1 and cost2.

4) Number of tamper-proof substantiate RTUs:

The maximum normalized attack impact versus the number of tamper-proof substantiate RTUs is figure out between NAMDIA and ARS SCADA. Attack impacts are evaluated at different costs (C1 and C2).

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 143-150

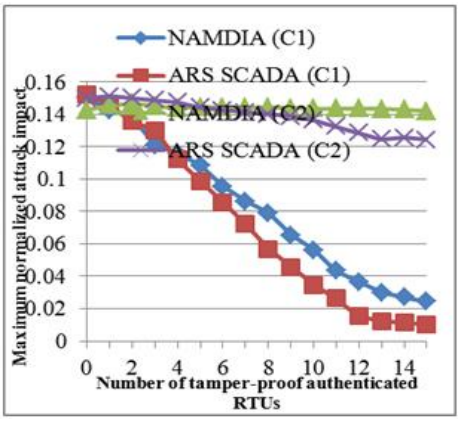

Fig. 6: Maximum normalized attack impacts versus the number of tamper- proof substantiate RTUs for cost 1 and cost2.

B. Latency:

Latency is intended with respect to two criterions 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 shown in Fig.7

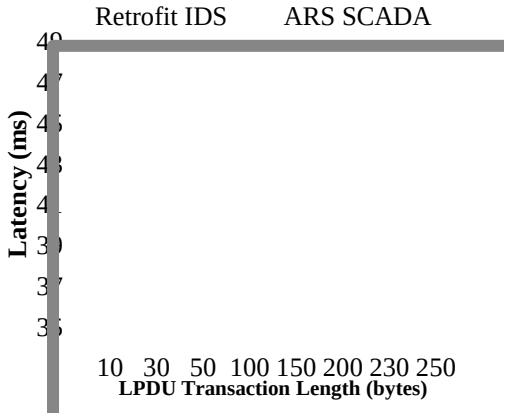

Fig. 7: Latency vs. LPDU length.

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.

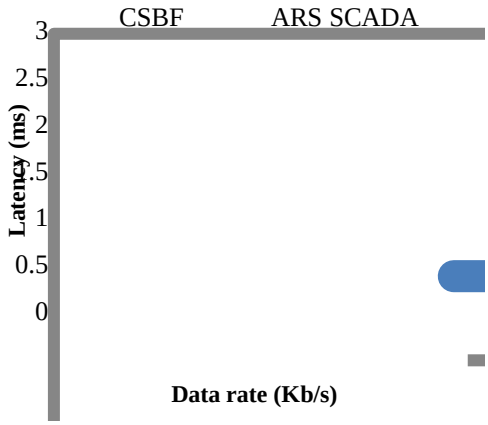

Fig. 8: Communication latency.

Conclusion:

Some Bottleneck infrastructures (BIs) are important owing to its global broadcasting area. The service dissemination of these systems changes radically when there is an attack. The consequence of these attacks may also be severe in disruption of other pivotal services. When the web based applications are merged with these control systems, the application becomes insecure and less bounded. The Low Powered Sensor Nodes (SNs) of a Wireless Sensor Network (WSN), Mobile Ad Hoc Networks (MANETs), and cyberspace are selected in this paper to contribute mobile operators and seize real time alerts. This work equips administration, portability, alert, collusion, detection and response. The ARS SCADA system is assessed in contrary to current modules like NAMDIA, retrofit IDS and CSBF for escalate the attack resistance and security of the SCADA systems. The achievement of the system is found good when compared with existing modules.

REFERENCES

Hull, J., 2012. "Staying in Control: Cyber security and the Modern Electric Grid," Power and Energy Magazine, IEEE, 10(1): 41-48.

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

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

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

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

Amin, S., 2012. "Cyber Security of Water SCADA Systems-Part I: Analysis and Experimentation of Stealthy Deception Attacks," Control Systems Technology, IEEE Transactions on, 99: 1-1.

Amin, S., 2012. "Cyber Security of Water SCADA Systems-Part II: Attack Detection Using Enhanced Hydrodynamic Models," Control Systems Technology, IEEE Transactions on, (99): 1-1.

Ericsson, G.N., 2010. "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure," Power Delivery, IEEE Transactions on, 25(3): 1501-1507.

Metke, A.R. and R.L. Ekl, 2010. "Security Technology for Smart Grid Networks," Smart Grid, IEEE Transactions on, 1(1): 99-107.

Amantini, A., 2012. "The human role in tools for improving robustness and resilience of critical infrastructures," Cognition, Technology & Work, 14(2): 143-155.

Dolgikh, A., 2012. "Using Behavioral Modeling and Customized Normalcy Profiles as Protection against Targeted Cyber-Attacks," in Computer Network Security, I. Kotenko and V. Skormin, Eds., ed: Springer Berlin Heidelberg, 7531: 191-202.

Alzaid, H., 2010. "A Forward and Backward Secure Key Management in Wireless Sensor Networks for PCS/SCADA," in Sensor Systems and Software, S. Hailes, S. Sicari, and G. Roussos, Eds., ed: Springer Berlin Heidelberg, 24: 66-82.

Alzaid, H., 2010. "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, pp: 859-865.

Hadžiosmanović, D., 2012. "A log mining approach for process monitoring in SCADA," International Journal of Information Security, 11(4): 231-251.

Vukovic, O., 2011. "Network-layer protection schemes against stealth attacks on state estimators in power systems," in Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, pp: 184-189.

Vukovic, O., 2012. "Network-Aware Mitigation of Data Integrity Attacks on Power System State Estimation," Selected Areas in Communications, IEEE Journal on, 30(6): 1108-1118.

Germanus, D., 2010. "Increasing the Resilience of Critical SCADA Systems Using Peer-to-Peer Overlays," in Architecting Critical Systems, H. Giese, Ed., ed: Springer Berlin Heidelberg, 6150: 161-178.

Barbosa, R. and A. Pras, 2010. "Intrusion Detection in SCADA Networks," in Mechanisms for Autonomous Management of Networks and Services, B. Stiller and F. Turck, Eds., ed: Springer Berlin Heidelberg, 6155: 163-166.

Morris, T. and K. Pavurapu, 2010. "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, pp: 958-963.

Fovino, I.N., 2012. "Critical State-Based Filtering System for Securing SCADA Network Protocols," Industrial Electronics, IEEE Transactions on, 59(10): 3943-3950.

Mander, T., 2010. "Power system DNP3 data object security using data sets," Computers & Security, 29(4): 487-500.