Middle-East Journal of Scientific Research 23 (9): 2318-2325, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.09.22715

Threat Modeling Framework for Electrical Distribution Scada Networks

[1]K. Immanuvel Arokia James and [2]R. Prabakaran

[1]Department of Information Technology, Vel Tech Multitech Engineering College, Chennai, India
[2]Department of Eee, Bit, Anna University, Trichirapalli, India

Abstract: SCADA (Supervisory Control and Data Acquisition) System has been the back bone of industrial automation. These systems are used to control and monitor industrial critical infrastructure functions such as electricity, gas, water, waste, railway and traffic. In the electrical domain SCADA systems have been widely installed for substation automation. The discovery of worm attacks that targeted the SCADA systems has raised the need for enforcing security measures in these systems. In this paper, the simulation environment to model the threats that attack SCADA distribution systems is proposed. The simulation environment enables the identification of cyber vulnerabilities, the impact of the exploits on controlled physical process and finally provides an assessment based on the criticality. The environment can also be used to develop cyber security mitigations. The drawback of these SCADA systems is that the threat modeling cannot be performed while the system is in execution and it can affect the electrical supply. The simulation environment provides the capabilities of modeling the existing threats and also tests the behavior of the system during potential attacks.

Key words: SCADA · Smart meter · Cyber Threat · OMNET++

INTRODUCTION

SCADA systems control and monitor the industrial and critical infrastructure functions. These systems have been deployed to control the distribution in a electrical network, to channel the flow of water systems such as potable water as well as waste water, to control the movement of railway traffic and also to control the oil distribution.

In the electrical domain, SCADA systems are installed in substations for remote control monitoring. In the initial stages of installation the security of these SCADA systems was established by the use of proprietary controls and isolated installations. For development of an intelligent distribution grid, there is a trend to interconnect the control network with the communication infrastructure ie the internet. Due to the increased connectivity to the internet the SCADA systems are vulnerable to the cyber attacks [1].

An attacker when gains access to the internal network of the substation control system can exploit particular aspects of the physical process such as altering the relay states. The impact of the attacks on substation is that it can halt the operation of the electrical distribution systems resulting in complete blackouts. The common threats that can cause the SCADA systems to malfunction are mostly man- in- the middle attacks. Here the critical control information is altered by the attacker and can thus manipulate the information to cause system instability.

Scada Networks for Distribution Automation: The development of a smart grid necessitates the integration of established SCADA networks with the existing corporate internet. The modern electrical grid is a communication network that links the various smart grid technologies such as Advanced metering Infrastructure, Demand Automation, Automated billing and so on.

Distribution automation (DA) optimizes a utility's operations and directly improves the reliability of its distribution power system. Adding targeted distribution automation capabilities can be economical when they are an extension of an existing SCADA investment and the communication infrastructure. The success or failure of an automation program depends on proper selection of equipment and communications to seamlessly integrate data into the utility control room.

Corresponding Author: K. Immanuvel Arokia James, Department of Information Technology, VEL TECH MULTITECH Engineering College, Chennai, India.

Scada Threats: The addition of the Distribution automation modules creates vulnerable access points in the smart grid network. These vulnerable points can become sources of cyber attacks. Apart from securing the systems from existing cyber related attacks, these systems must be protected from cyber attacks that are specifically designed to bring down the power network [2].

The currently operating SCADA systems are legacy systems that were setup for functioning for a long period of time. In order to add security, these systems cannot be built again from scratch as it is highly costly and the losses due to the system outage are very high. Hence security must be added as a workaround without bringing down the system.

The increased complexity of the modern SCADA systems exposes them to a large number of implementation flaws that can be utilized by the exploiters to gain access to the control network of these systems. The modern SCADA systems have to be connected to the corporate or other networks. This has to be done so that business can operate more efficiently and enable business leaders to track and control production in real time and react immediately for any problems that can arise during production. In such a networked system, an exploiter need not be physically present in the plant facility to bring down the system. The attacker can gain entry into the system by making use of the vulnerabilities in the gateway between the system and network.[3]

Related Work: The research on SCADA security has been carried by other authors which has been mentioned below. In the paper' *SCADASim-A Framework for Building SCADA Simulations'* [4] authors have developed a modeling simulation tool that would enable the simulation of SCADA systems with the benefit of testing different attack and security solutions. The simulation tool built supports the integration of external devices and applications. The main advantage is the ability to test the effect of attacks on real devices and applications even though using simulated environment. In another work carried out by Chabukswar et al '*Simulation of Network Attacks on SCADA Systems'* [5] here have used the Command and Control WindTunnel infrastructure which is an integrated, graphical, multi-model simulation environment which can be used to simulate heterogeneous systems such as the SCADA network. This framework enables various simulation engines to interact and transmit data to and from one another and log and analyze the real time simulation results. Another work '*EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation'*[6] was developed by the authors for cyber physical security study. The EPIC is a modern scientific instrument that can provide accurate assessments of the impact that cyber-attacks may have on the cyber and physical dimensions of Networked Critical Infrastructures(NCI). EPIC uses an emulation testbed based on Emulab to recreate the cyber elements of a NCI and software simulators for the physical components. When compared to other testbeds its main advantage is that it can support very accurate, real-time, repeatable and realistic experiments with heterogeneous infrastructures. This powerful scientific instrument can be used to study multiple interdependent infrastructures and provide insights about the propagation of faults and disruptions. In a similar work carried out by Govindarasu et al [7] have developed a smart grid security testbed, including the set of *control*, *communication* and *physical system* components required to provide an accurate cyber physical environment. It then identifies various testbed research applications and also identifies how various components support these applications. The authors have developed Power Cyber testbed which support the capabilities such as virtualization, Real Time Digital Simulators (RTDS) and ISEAGE WAN emulation. The Power-Cyber cyber-physical testbed integrates industry (SCADA) hardware and software along with emulation and simulation techniques to provide an accurate electric grid cyber infrastructure. The testbed employs virtualization technologies to address scalability concerns and reduce development cost.

Advanced Metering Infrastructure (AMI) in Distribution Automation: The traditional meters which are either analog or digital are used to record the usage of the consumer and the usage is billed by the utility companies. Thus the metering infrastructure was a one way communication. The AMI or the smart meters are deployed at the consumer location. With the help of this smart meter the utilities are able to collect information from the consumers immediately in response to consumer needs as shown in Fig. 1. The information provides the necessary details such as household energy usage.

Smart Meter Benefits: The AMI installations provide wide benefits which were not possible originally with the traditional one way technologies such as increased energy conservation as shown in the fig, remote meter recordings, service faults and outage detection. The meters operate under safe EM emission standards as highlighted in Fig. 2.

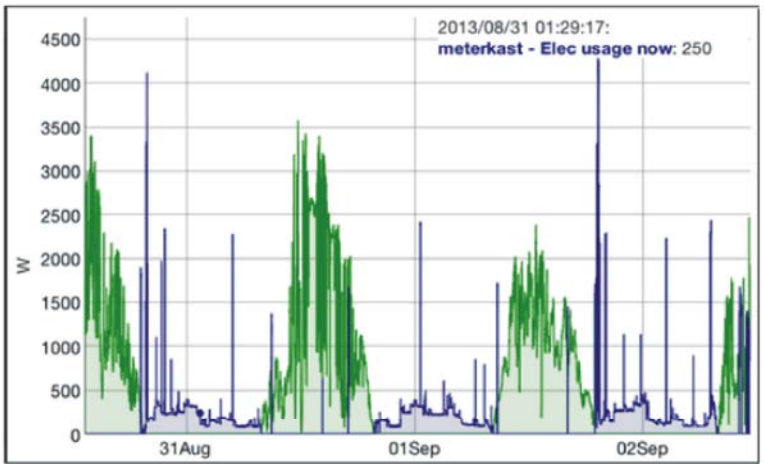

Fig. 1: Consumer response analysis

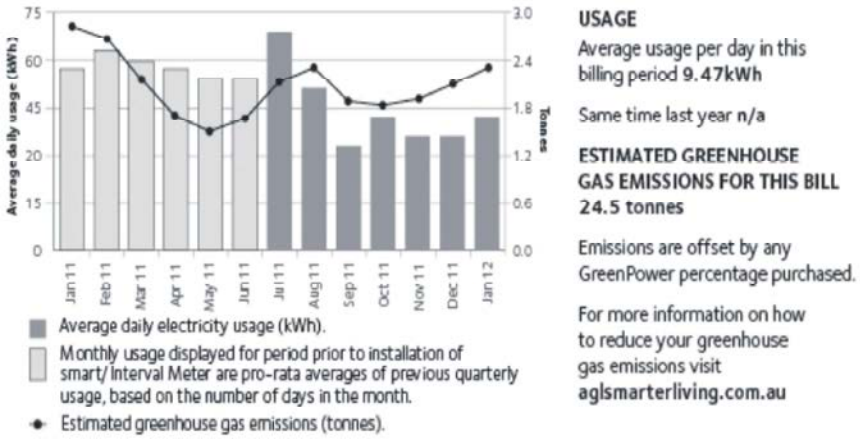

Fig. 2: Energy conservation survey

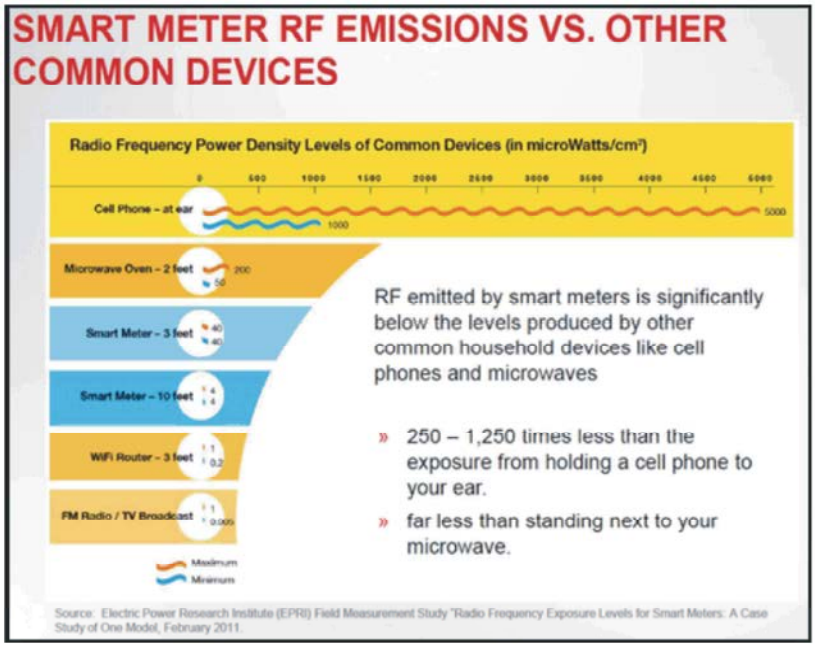

Fig. 3: EM emission standards

Cyber Threat Possibility in Distribution Automation: IT penetration in Indian Distribution sector for control and operation is relatively low. These are presently concentrated in MIS, Metering and Billing. Distribution systems operations are increasingly being centralized and any cyber incidence at Central Location can cause power supply failure. A disruption to critical infrastructure/customers like Hospitals, Metro and Railways etc is of strategic concern. Interruption / wrong reporting in data collected through Automatic Advanced Metering Infrastructure (AMI) may result wrong/non operational decision and revenue losses.

Smart Meter as a Source of Attacks: The smart meters are deployed for implementation of automated metering reading (AMR), automated metering infrastructure (AMI) and smart grid infrastructure [9]. Due to the increased deployments the security attacks like data hacking, introducing malware in the system and other cyber attacks are on the rise. A smart meter without security installation has the potential for introducing many risks.

The risks range from low to high category with respect to the utility. Risks such as monitoring the data transfers from consumer to control center will be under low risk. The data can be misused to know the details of the presence of consumer at residence. Thus a unsecured meter data transmission possess serious privacy invasion issues. Medium risk can be one such as the billing information is forged to cause subsequent revenue losses. Finally the higher risk is one in which the attacker is aware of the operation of the Electrical Distribution and modifies the control data to cause intentional power failure. Thus the meter can be used as a tool to access the critical distribution network and can be used to send false data. Thus a smart meter can be a vulnerable point to intentionally cause damage to infrastructure and economic losses.

Modelling of the Cyber Threat: In order to develop a security architecture for the distribution network; the environment must be first developed for studying the attacks and well as modeling future attacks. The already available networking tools can be utilized to create the threat environment [10].

OMNET++: OMNeT++ is a discrete event simulation framework focusing on computer network simulations. OMNeT++ is an open source tool and allows users extensive low-level control over its scheduling algorithm used and other simulation details. The simulated network can be designed using the provided graphical interface or by manipulating simulation files in OMNeT++'s custom scripting language, NED. Network modelers must define the nodes in the network, the messages types that can be passed among them, the connections between nodes and any configuration parameters needed by the included nodes. SCADA simulations can use OMNeT++ to model a control network in a SCADA system.

INET Framework: INET Framework contains IPv4, IPv6, TCP, SCTP, UDP protocol implementations and several application models. The INET Framework supports wireless and mobile simulations as well. Protocols are represented by simple modules. A simple module's external interface (gates [connectors] and parameters) is described in a NED file and the implementation is contained in a C++ class with the same name. Some examples are TCP, IPv4. These modules can be freely combined to form hosts and other network devices with the NED language.

NETA Framework: The NETA framework uses the same idea as OMNeT++, i.e., modules that communicate by message passing. The general idea of the present framework is to develop new nodes which can strike attacks. In order to do this, the implemented attacks are managed in what we called attack controllers. These controllers affect to one or more modules of INET framework through control messages sending parameters of the developed attacks. Therefore, these modules should be conveniently modi?ed to obey the orders of the control messages. These modi?ed modules are named hacked modules.

In Fig 5. we can see the comparison between a normal node and an attacker node. The normal node is composed of simple and compound modules which communicate between them. The attacker node is composed of the same number of modules and its communications and the attack controller modules. However, some modules have been substituted by the correspondent hacked modules to allow the execution of the attacks trigger by the included attack controllers.

System Description: The SCADA system that will be developed for simulation consists of a four field devices that are controlled from a remote location. The control center and the remote substation are linked through the internet. The attacker node that is used to create attacks will be linked to the SCADA network through the internet. The system block diagram is as below:

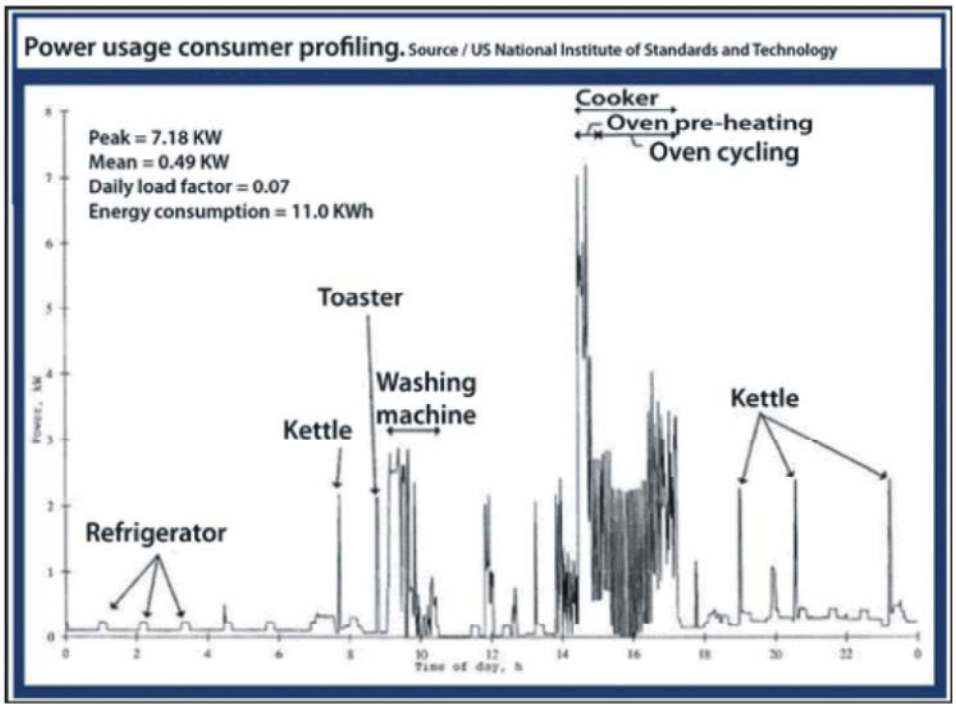

Fig. 4: Power consumer profiling

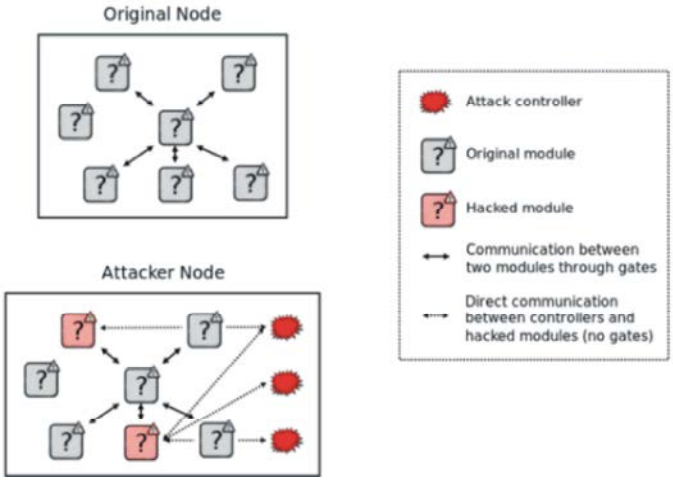

Fig. 5: Comparison between normal mode and attacker node

Attack Model: The following cyber threat scenarios are modeled in the OMNeT tool.

- Denial of service attack
- Forging the metering information
- Modification of control information

Denial of Service Attack: In this attack scenario the attacker node tries to disable the network communication flow. This can be modeled as the following attacks:

Flooding Attack: In this class of attack, the attacker nodes flood the network with dummy packets so that the communication flow is interrupted.

Drooping Attack: In the IP dropping attack, nodes exhibiting this behavior intentionally drop, with a certain probability, received IP data packets instead of forwarding them, disrupting the normal network operation. Depending on the application, it can turn the network much slower due to the existence of retransmissions; make the nodes waste much more energy resources, etc.

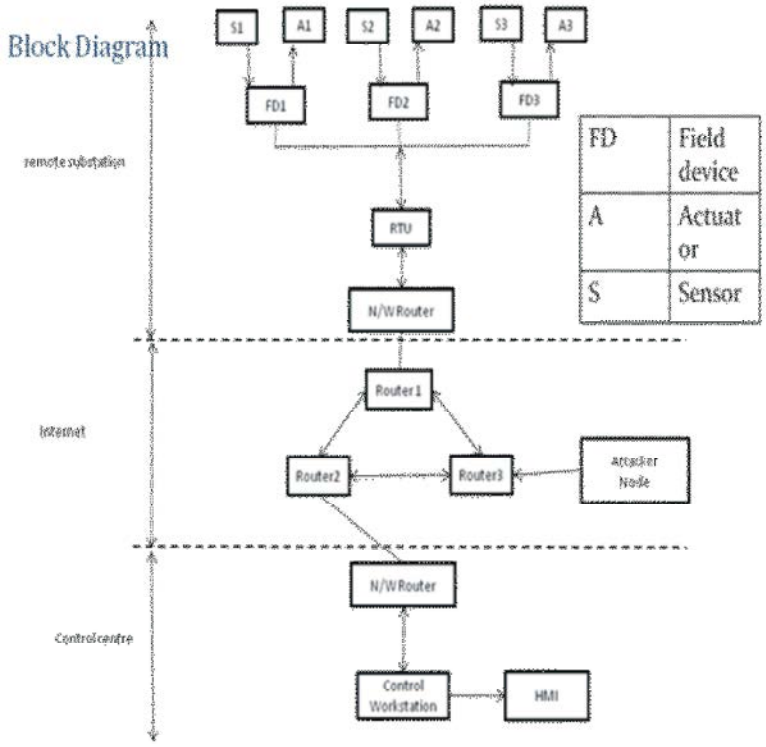

Fig. 6: System block Diagram

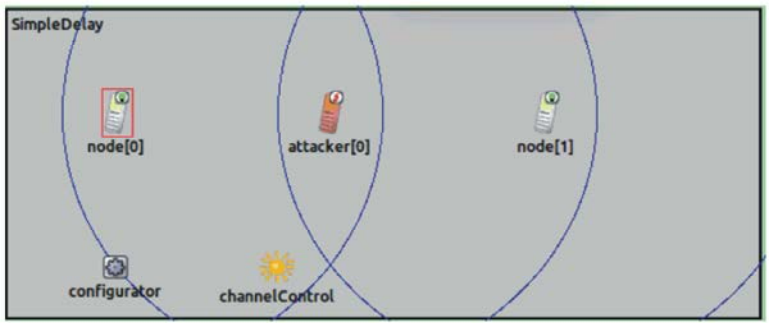

Fig. 7(a): Simulation Results

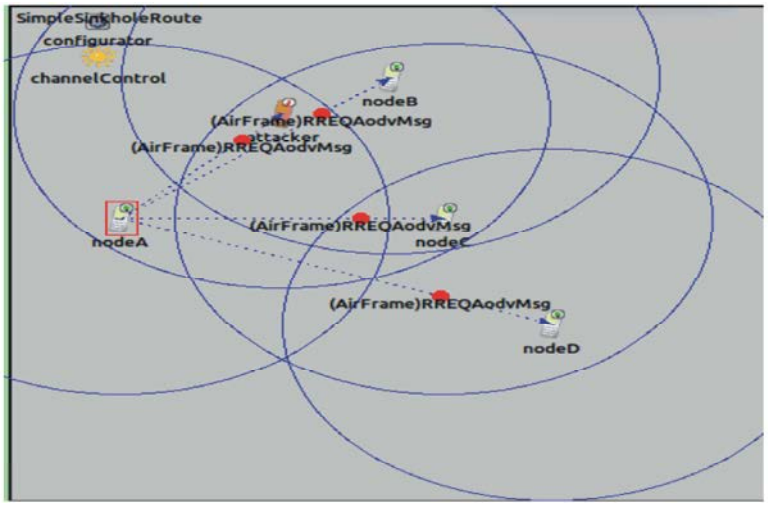

Fig. 7(b): Simulation Results

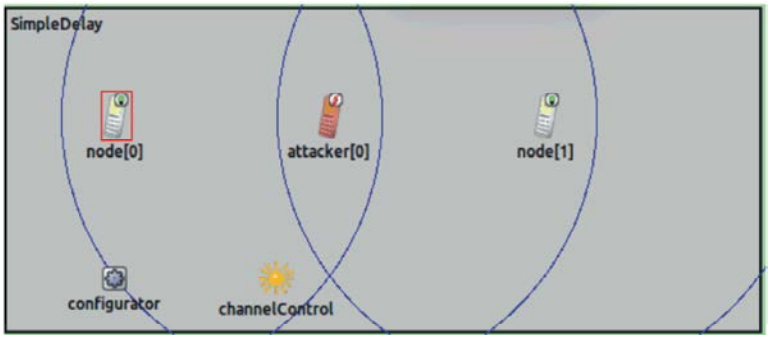

Fig. 7(c): Simulation Results

Sinkhole Attack: In a sinkhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causing other nodes to route data packets through itself. Here, the attacker forges routing replies (RREP) to attract traffic.

Delay Attack: In this attack, a malicious node delays IP data packets for a certain amount of time. This can affect different QoS parameters (end-to-end delay, jitter, etc.), resulting in a poor network performance.

Forging the Metering Information: Here the attacker node modifies the billing information and sends the false data to the data servers.

Control Data Modification Attack: The attacker node captures the packet with control information and modifies the original information. This causes irrelevant changes in the system and thus can cause damage to the connected components. If suppose the control information was to shut down certain areas for maintenance and if the modified data causes come other regions to shut down, then it will cause damage to human life and property.

Conclusion and Future Work: Thus the paper highlights that the automation in electrical distribution is essential for seamless delivery of electrical power. The smart meter is a key technology for achieving the smart grid. The efficient implementation requires that security must be built in into the system. The security aspects must be upgraded in the interface devices that link the corporate network with the control network. Other measures of security being using secure protocols, restricted server access, timestamp for messages and hardware based security. Future work includes developing a secure architecture for the interface devices.

REFERENCES

1. Chen, T.M.; Abu-Nimeh, S., "Lessons from Stuxnet," Computer, 44(4): 91-93.
2. Fadi Aloula, A. R. Al-Alia, Rami Al-Dalkya, Mamoun Al-Mardinia and Wassim El-Hajjb, 2012. 'Smart Grid Security: Threats, Vulnerabilities and Solutions', International Journal of Smart Grid and Clean Energy.
3. Almalawi, A., Z. Tari, I. Khalil and A. Fahad, 2013. "SCADAVT-A framework for SCADA security testbed based on virtualization technology," Local Computer Networks (LCN), 2013 IEEE 38th Conference on, pp: 639-646, 21-24 Oct. 2013
4. Queiroz, C., A. Mahmood and Z. Tari, "SCADASim-A Framework for Building SCADA Simulations," Smart Grid, IEEE Transactions on, 2(4): 589-597.
5. Chabukswar, R., B. Sinopoli, G. Karsai, A. Giani, H. Neema and A. Davis, 2010. "Simulation of Network Attacks on SCADA Systems," First Workshop on Secure Control Systems, Cyber Physical Systems Week 2010, April 2010
6. Siaterlis, C., B. Genge and M. Hohenadel, 2013. "EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation," Emerging Topics in Computing, IEEE Transactions on, 1(2): 319-330. Dec. 2013 doi: 10.1109/TETC.2013.2287188.
7. Sridhar, S., A. Hahn and G. Manimaran, 2012. "Cyber-physical system security for the electric power grid," Proceedings of the IEEE, 100(1): 210-224.
8. Ye Yan, R.Q. Hu, S.K. Das, H. Sharif and Y.I. Qian, 2013. "An efficient security protocol for advanced metering infrastructure in smart grid," Network, IEEE, 27(4): 64-71.

9. White paper by Meera Balakrishnan, Freescale semiconductors,' Security in Smart Meters'.
10. Chinnow, J., K. Bsufka, A.D. Schmidt, R. Bye, A. Camtepe and S. Albayrak, 2011. "A simulation framework for smart meter security evaluation," Smart Measurements for Future Grids (SMFG), 2011 IEEE International Conference on, pp: 1, 9, 14-16.