The Journal of CPRI,
Vol. 11, No. 1, March 2015 pp. 79-92

Transient analysis of cyber-attacks on power SCADA using RTDS

Abhiram Amaraneni*, Mahendra Lagineni*, Rajesh Kalluri*,
Senthilkumar R K* and Ganga Prasad G L*

Cyber security in the SCADA domain has become one of the major concerns of all the stakeholders in the energy sector. The SCADA architecture that the power industry adopts is drawing more attention from a dedicated cyber attacker due to the extent of damage a catastrophe can promise. The usage of open standard protocols for communication among SCADA components that are not designed with security in mind is one of those vulnerable areas for any attacker. The SCADA components in the control region viz., the MTU and the RTU communicate via these insecurely designed open protocols without any authentication. An attacker can target this communication; launch an attack like the man-in-the-middle attack resulting in a disastrous situation. An experiment was conducted at CPRI using their Real Time Digital Simulator (RTDS) simulating a substation to study the impact of an attack. This paper brings out the details of the experiment conducted and the results thus obtained.

Keywords: *SCADA, RTU, MTU, RTDS, IEC 60870-5-104/101 protocol& vulnerabilities, cyber-attack.*

1.0 INTRODUCTION

SCADA is the acronym of Supervisory Control and Data Acquisition, which is used for remote monitor and control of many control systems [1]. SCADA system was introduced for local systems in the beginning, whose application has been expanded to wide area systems as the technology evolves. Today SCADA technology is widely used in utility sector for its data acquisition and process control. SCADA packages are available or can be tailored for applications to many processes such as [2]: water supply, irrigation system, sewage lift station, oilfield and pipeline control, power generation/transmission automation (Energy Management System or EMS), power distribution system (Distribution Management System or DMS), system control of communication network (SYSCON), security system, early warning siren system, mass transit system, etc.

SCADA systems are mainly composed of three components such as Remote telemetry unit (RTU), Master terminal unit (MTU) and communication links. Field devices are connected to RTU over RS232 and RS485. RTU acquires data from field devices and acts as a data concentrator [3]. MTU communicates with the RTU over the communication links adhering to the protocol agreed upon by RTU and MTU. Each MTU may communicate with multiple RTUs based on the requirement. Human machine interface (HMI) [4].

Communication links between MTU and RTU could be composed of different ways such as radio, microwave, spread-spectrum, twisted-pair, fiber-optics, dial-up, leased line, etc. The IEEE standard C37.1-1994 specifies the communication topologies used in SCADA [5]. They vary from a simple point-to-point to composite architectures with one single master station, multiple sub-

*Real Time Systems & Smart Grid Group, Center for Development of Advanced Computing, No. 1, Old Madras Road, Byappanahalli, Bengaluru - 560038, India. E-mails: {aabhiram,laginenim,rajeshk,senthil,gpr}@cdac.in

master (slave master) stations and multiple RTUs. The topology of SCADA network depends on the objective and characteristics of the controlled system such as the control governance, the data type, the required communication speed, etc. SCADA and other control systems have several standards for their data communication, called protocols. They define physical media, communication procedures, data frame, etc.

The SCADA system protocols evolved from proprietary hardware and software designed specifically for SCADA systems. But, with proprietary protocols interoperability is a critical issue. Currently, there is a wide variety of open standard protocols adopted between MTU and RTU. Some of the open standard protocols are IEC 870-5-101, IEC 870-5-104, Modbus, DNP3 etc. Adhering to standards, MTU can acquire data from RTU as well as can issue control commands to control field devices using RTU. Convergence of SCADA systems and control networks into conventional IT systems has widened the SCADA Security's vulnerability spectrum. Open systems, standards and improved connectivity with other systems have added to the security concerns.

The rest of the paper is organized as follows: Section 3 gives a brief introduction to the communication protocol IEC60870-5-104 and its vulnerabilities. Section 4 discusses the experiment setup and the components. Section 5 outlines the steady state simulation. Section 6 discusses two transient simulation cases with the experiment results. Section 7 concludes the paper summarizing the findings of the results.

2.0 IEC 60870-5-104/101 PROTOCOLS AND THEIR VULNERABILITIES

A. Protocol introduction

IEC 60870-5-104 is an Ethernet based protocol used for telecontrol (SCADA) in electrical engineering and power system automation applications. It is a protocol used for communication in the control region of SCADA *viz.,* between MTU and RTU devices. The protocol uses a similar frame format used by IEC 60870-5-101 (a serial line protocol) [6] but uses an open TCP/IP interface to have connectivity to LAN.

The frame format of IEC 60870-5-104 has two parts in it *viz.,* Application Protocol Control Information (APCI) and Application Service Data Unit (ASDU). The ASDU part is all concerned with the actual information being transferred and its metadata. The same is also shared by IEC 60870-5-101 protocol. The APCI is 6 octets in length and contains a start character, the specification of the length of the ASDU and 4 octets of the control field [7]. IEC 60870-5-104 protocol supports various types of data to be exchanged between MTU and RTU such as, analog/digital data acquisition from RTU, control commands from MTU, transfer of files, time synchronization, etc. Of these, data acquisition and control commands form the core of the communication.

B. Vulnerabilities:

IEC 60870-5-104 communication is more vulnerable than IEC 60870-5-101 communication at transport and network layers due to the former's adoption of TCP/IP. But the application layer vulnerabilities are at the same level [8]. Following is a detailed analysis of IEC 60870-5-104 vulnerabilities:

1) Vulnerabilities due to the communication channel.

2) Vulnerabilities in the protocol due to the lack of inbuilt security mechanisms.

1) IEC 60870-5-104 protocol work on TCP/IP communication. A plain TCP connection may be attacked in a variety of ways resulting in unwanted/compromised situations like the following:

a) Denial of service: Denial of service is a situation where large amounts of resources in the network and server are consumed due to flooding of packets from an attacker using a spoofed IP address [9].

b) *Connection hijacking:* By eavesdropping a TCP session an attacker can redirect packets and hijack a TCP connection. An attacker uses some ways of predicting the sequence numbers from the ongoing communication and sends his own packet with the new sequence number. When this packet gets acknowledged to the other side of the connection, synchronization is lost. This method can be combined with ARP attack to take a permanent control of the hijacked TCP connection [10].

c) *TCP veto:*An attacker, who can eavesdrop into the communication and can correctly predict the sequence number and the size of the next packet to be sent, can inject a malicious packet. Since the packet with the correct sequence number and payload size is already received, the genuine packet sent by the sender will be ignored by the receiver. This is relatively less effective but remains highly undetectable [11].

2) Due to no special care taken to provide security in the protocol, IEC 60870-5-104 communication is always vulnerable for attack on its:

a) *Confidentiality:* Since this is a plain text communication, it is easy for an eavesdropper to have access to the actual data being transferred. The protocol, being an open standard, makes it easier for an attacker to interpret the packets appropriately.

b) *Integrity:* For an attacker who is successful in launching a man-in-the-middle attack, with enough knowledge about the protocol, can modify the packet in its transit to MTU to indicate wrong measurement values and incorrect status of the devices. This can in turn force the operator to take an inappropriate action.

c) *Authenticity:* The protocol has no provision to authenticate the communicating device. This makes it possible for an intruder to inject a packet to send it to RTU. The injected packet can have a command to perform a task that results in a catastrophic situation in substation [12].

There are others threats like replay attack and non-repudiation. While replay attacks can be countered, only to an extent and not completely, by an effective use of the sequence numbers that inherently feature in the protocol, non-repudiation doesn't fall in the same threat level that is being discussed in this paper.

3.0 EXPERIMENTAL SETUP

With all the vulnerabilities mentioned in the last section it is to be concluded that the SCADA network is not immune to a cyber-attack. Now, the consequence of any such cyber-attack also has to be established. For this purpose, an experiment has been conducted at CPRI by using its RTDS facility to simulate the Salem substation as shown in Figure 1. The goal of the experiment is to bring out how a cyber-attack affects the SCADA network.

A. SCADA network:

The SCADA network consists of an MTU developed by C-DAC to interact with the RTU. The system also hosts an HMI to display the data acquired from the RTU. This MTU machine is in LAN connection with another system that can be used as historian, reporting system etc. The MTU, with the help of a router connects to RTU which is in a different network.

B. RTU:

RTU is configured to process 20 measurand values (analog input) for inputs and 13 indication signals (digital) for both input and output. The analog inputs were configured for measurement ranges of 0-10V. The RTU, when connected to the RTDS, senses the analog electrical signals at the connected points and converts them to digital information (using 15 bit ADC) before passing it to the MTU. The digital inputs were configured for measurement ranges of 0-48V where ~0V is considered as logical 0 and ~48V as logical 1.

C. RTDS:

The RTDS is a special purpose computer designed to study Electromagnetic Transient Phenomena in power systems in real – time. The RTDS comprises of specially designed hardware and software. RTDS hardware is Digital Signal Processor (DSP) based and utilizes advanced parallel processing techniques in order to achieve the computation speeds required to maintain continuous real-time operation.

D. Modeling of Salem system on RTDS:

Modeling of Salem system on RTDS is carried out considering the system data given in Figure 2. This is real time information provided by SRLDC, Bangalore.

Incoming lines to Salem substation are from Bangalore (BNG), Hosur (HSR), Neyveli circuit I (NYLI) & Neyveli-circuit2 (NYLII). The infeed to Salem substation is around 810MW. This power is meeting the load demand at Myvadi through Myvadi circuit-I and Myvadi circuit-II (UPTII) and local load through ICTs.

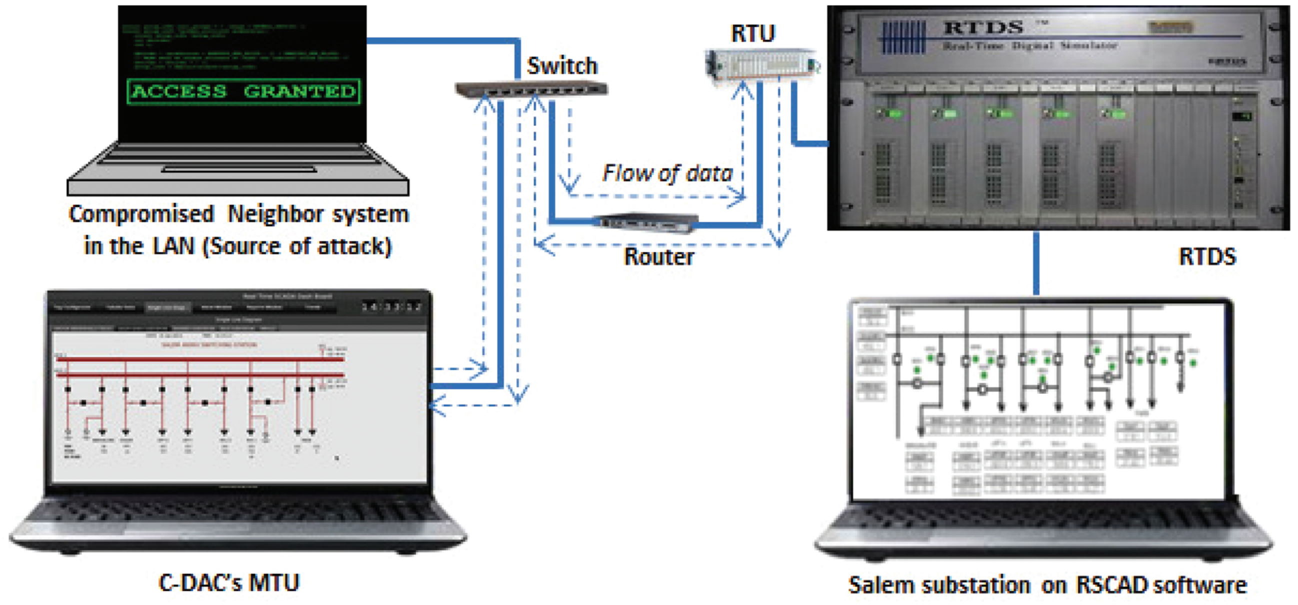
ACCESS GRANTED
Switch
RTU
RTDS
Flow of data
Compromised Neighbor system in the LAN (Source of attack)
Router
RTDS
C-DAC's MTU
Salem substation on RSCAD software

FIG. 1 EXPERIMENTAL SETUP AT CPRI

Power flow through incoming and outgoing lines is given in Table 1 below. This system is modeled in RTDS with the help of RSCAD software.

TABLE 1

POWER FLOWS ON CONNECTING LINES TO SALEM SUBSTATION

Incoming Lines	**P in MW**	**Q in MVAR**
Bangalore to Salem	147	-57
Hosur to Salem	319	-58
NYL-I to Salem	169	73
NYL-II to Salem	175	19
Total Power	**810**	**-23**

Outgoing Lines	**P in MW**	**Q inMVAR**
Myvadi-I (UPT-I)	-343	72
Myvadi-II(UPT-II)	-335	79
ICT-I(TNEB)	-18	-21
ICT-II(TNEB)	-111	-35
Total Power	**-807**	**95**

Synchronous machine data, transmission line data, load data and reactor data are configured as per the requirements.

4.0 STEADY STATE SIMULATION

Steady state simulation of the Salem substation is carried out in RTDS with the power flows matching with the snap shot of the power flows given in Figure 2. The single line diagram of the system represented on RTDS with Real time simulation of bus voltage, active power and reactive power read by RMS meters is given in Figure 3.

Voltages of the incoming lines, Real and Reactive power flows of incoming lines, Frequencies are given in Figure 4. Voltages of the outgoing buses, Real and Reactive power flows on outgoing lines, Frequencies are given in Figure 5.Voltages of the incoming lines are nothing but the voltages at terminal buses they are modeled by generators. All the values are steady state values. Breaker signals from RTU are recorded and shown in Figure 6. All signals are high indicating the breakers are closed in steady state condition.

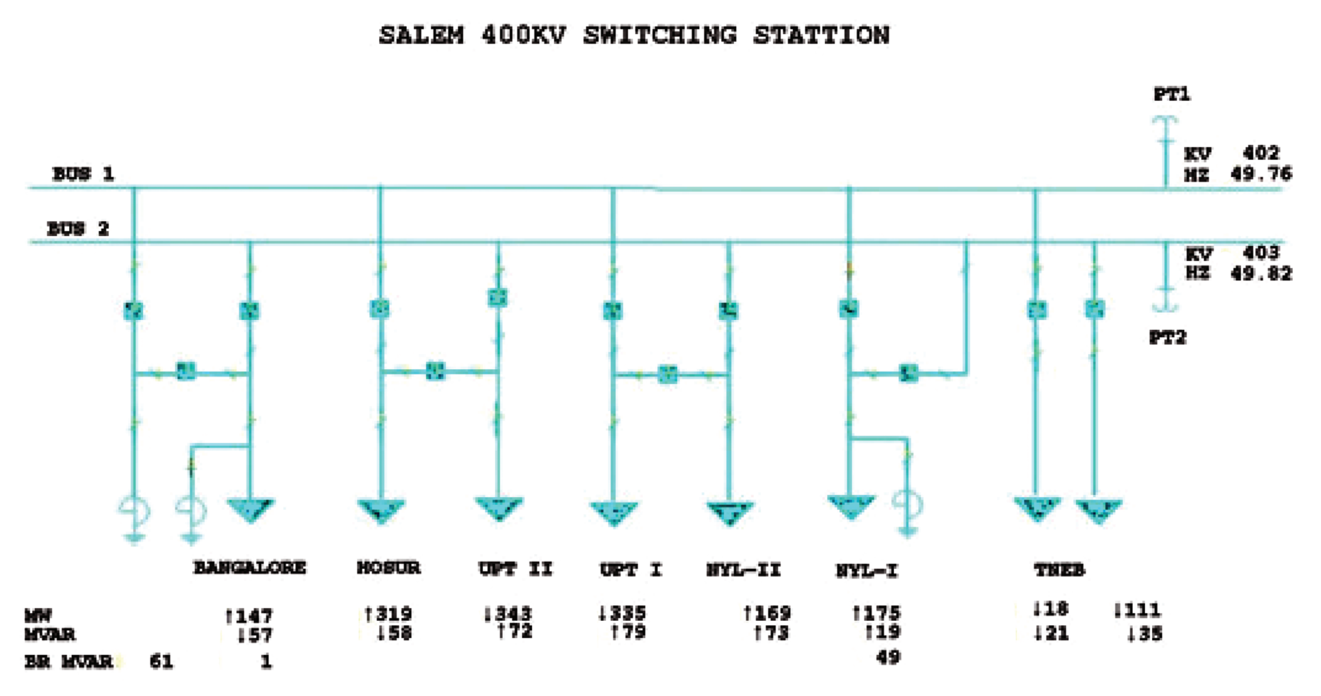

FIG. 2 SINGLE LINE DIAGRAM OFSALEM SUBSTATION

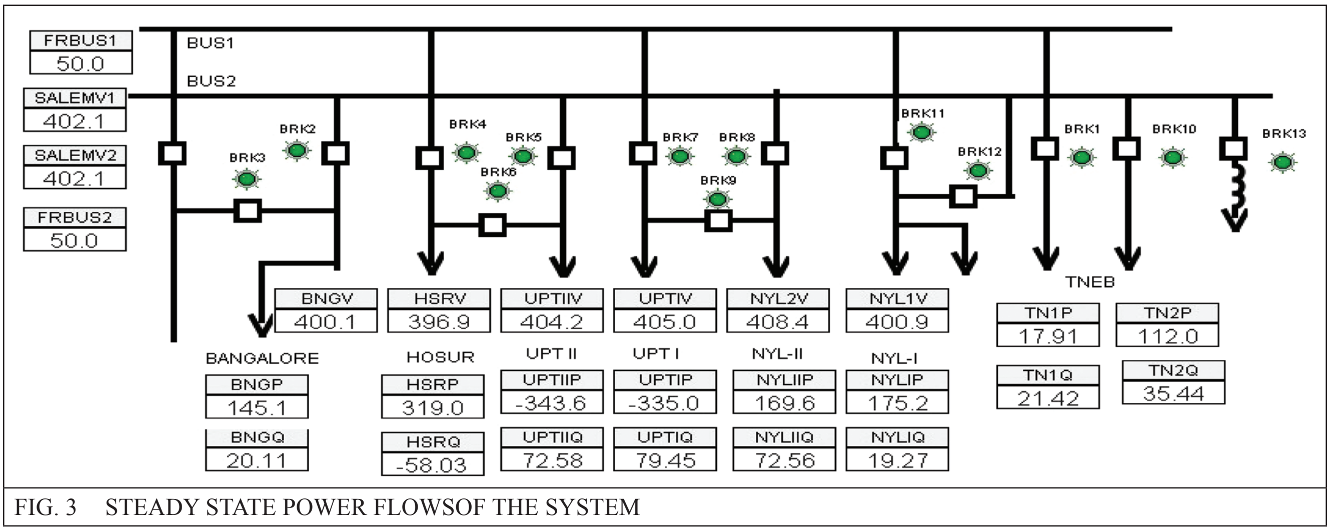

FIG. 3 STEADY STATE POWER FLOWSOF THE SYSTEM

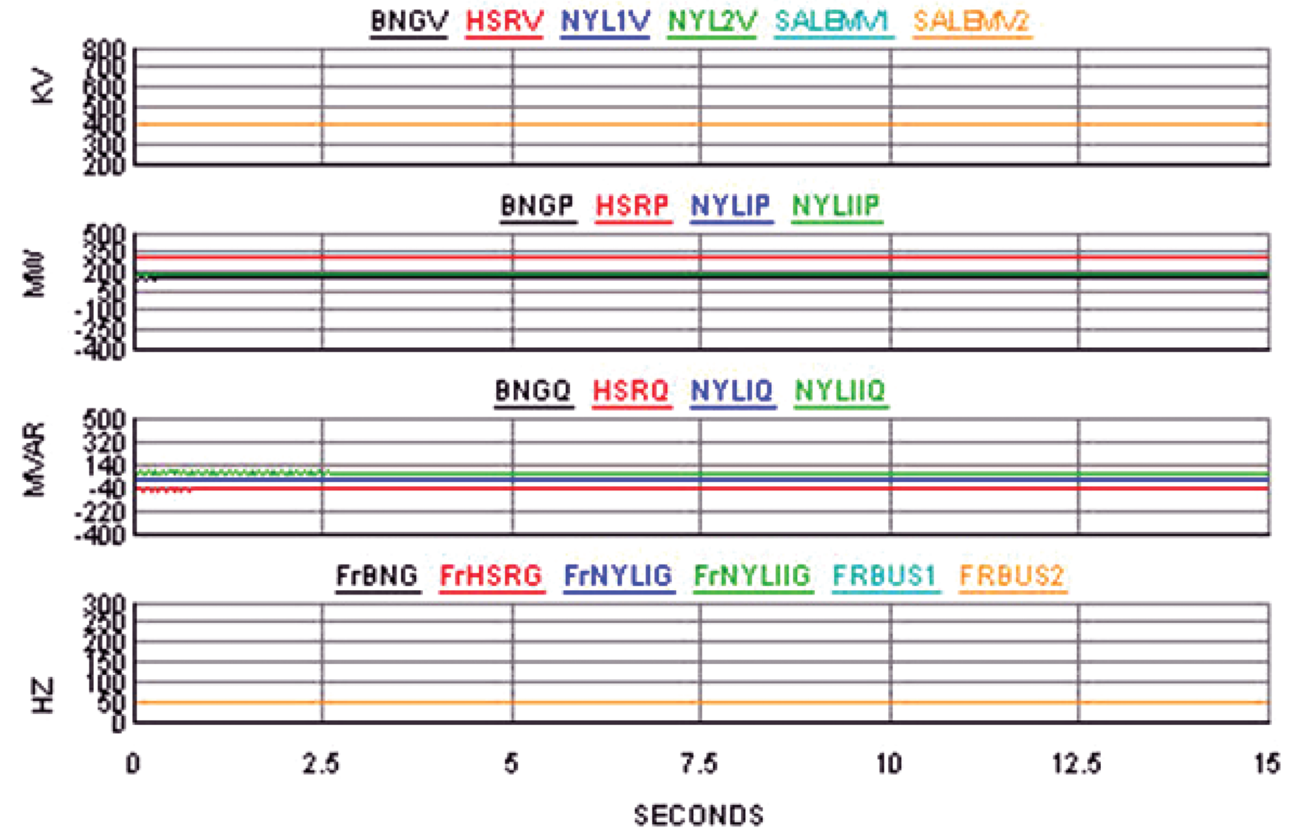

FIG. 4 STEADY STATE – VOLTAGES, P & Q FLOWS, FREQUENCY ONINCOMING LINES

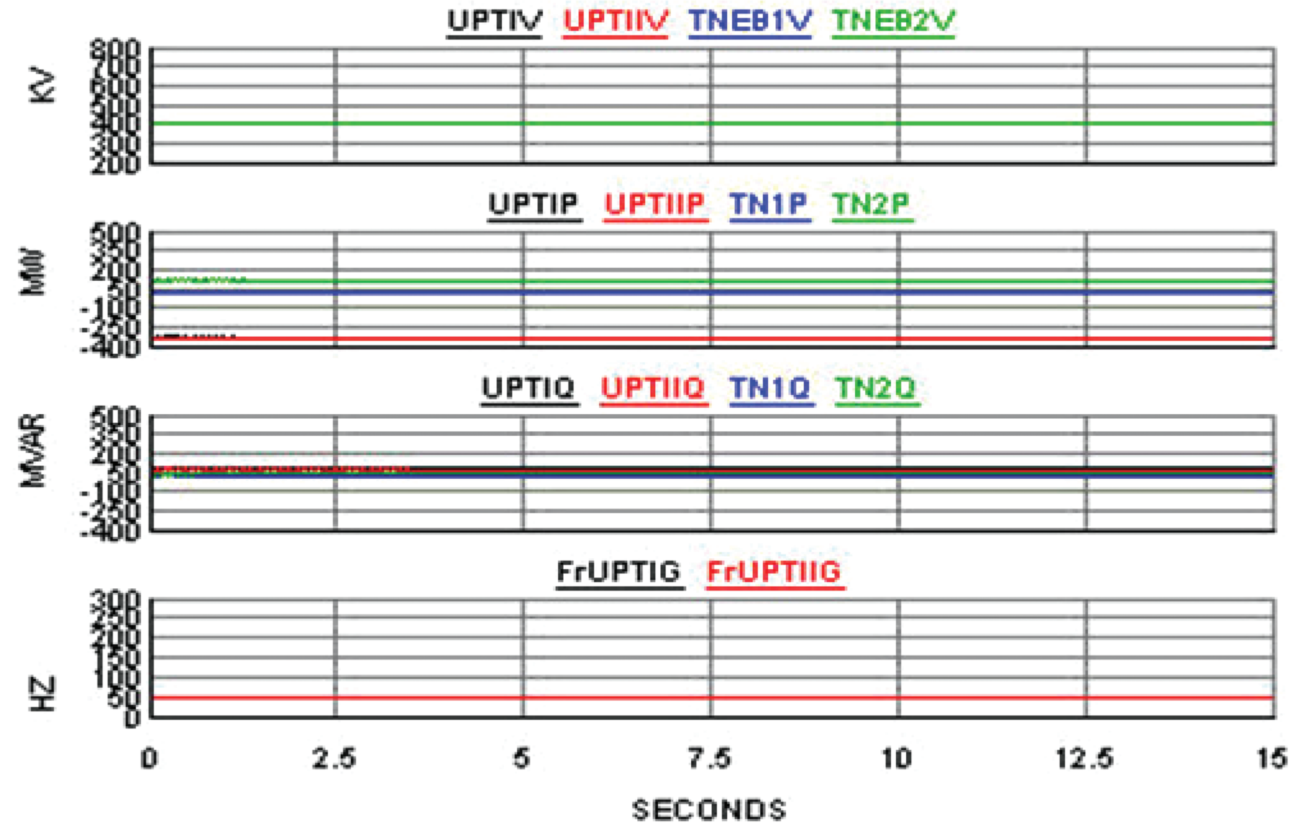

FIG. 5 STEADY STATE – VOLTAGES, P & Q FLOWS, FREQUENCYON OUTGOING LINES

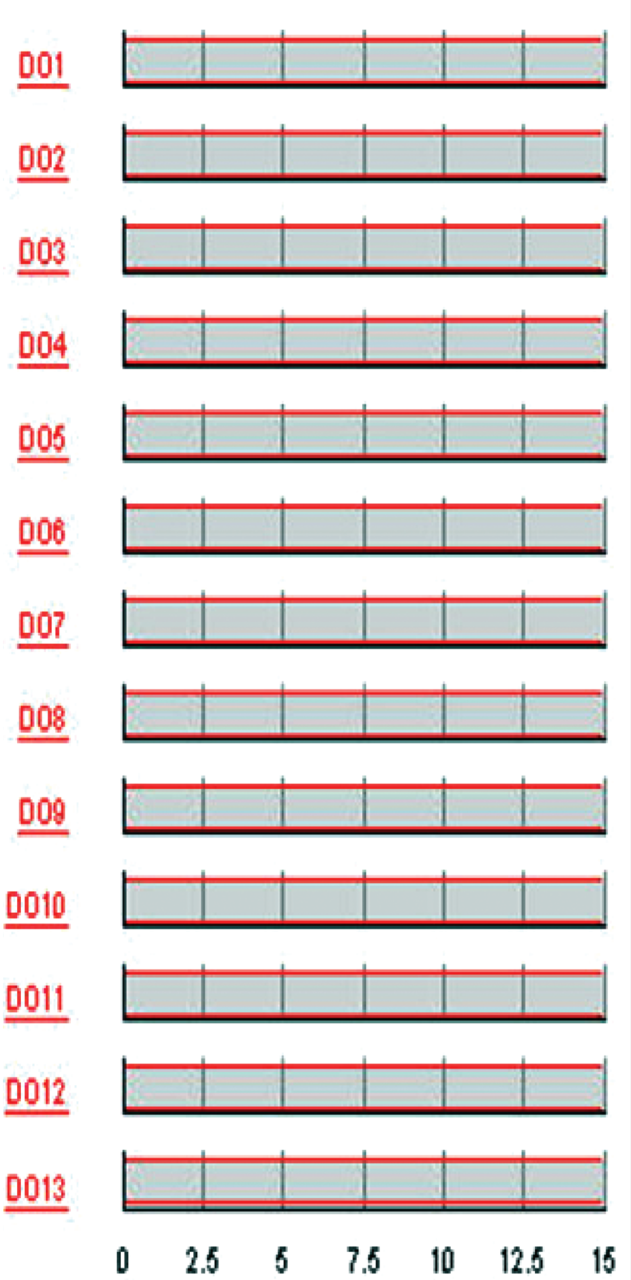

FIG. 6 STEADY STATEBREAKERSIGNALSFROM SCADA SYSTEM

5.0 TRANSIENT SIMULATION CASES

Transient simulation cases are carried out as attacks by the compromised neighbor system in the same network of MTU. Using C-DAC's in-house hacking tools, the compromised system is successfully able to launch a man-in-the-middle attack to route the network traffic between the MTU and RTU through it. The details of the attack are beyond the scope of this paper.

Once it is made sure that the traffic is routed through his system, the hacker can either passively look at the data flowing or indulge in data modification. The attacker can also initiate a command to the RTU. Several attack experiments have been carried out on the simulated Salem substation and the results have been captured using RTDS for impact analysis. Among them, two such attack cases have been presented below.

A. Sending command to Hosur and Neyveli II breakers and Tie breakers by the attacker:

In this attack, the attacker initiates a command from his machine. The intention is to bring down some of the field devices to make the substation unstable.

Healthy system data (steady state data):
Hosur:
Source MW: 319 MW, *Breaker:* ON,
Tie-Breaker: ON, *Bus voltage:* 396.9kV
Frequency: 50.0Hz
Neyveli II:
Source MW: 169.6 MW, *Breaker:* ON,
Tie-Breaker: ON, *Bus voltage:* 408.4kV,
Frequency: 50.0Hz

The attacker initiates a command to the RTU to make the line breakers (BRK4 & BRK8) and Tie breakers (BRK6 & BRK9) off. This is a direct attack from the attacker to make the substation unstable. As evident from Figure 7, MW of the incoming lines Hosur and Neyveli II are dropped causing instability in Salem substation.

The bus voltages and frequencies of the substation behave abnormally and the system is unstable as can be seen in Figure 7. Breakers 4, 6, 8and 9 signals are becoming 'LOW' showing the attack and all other breaker signals are 'HIGH'. Parameters of the incoming and outgoing lines are going abnormal as can be seen from Figure 8 and Figure 9 respectively. Breaker signals from SCADA system are recorded and shown in Figure 10.

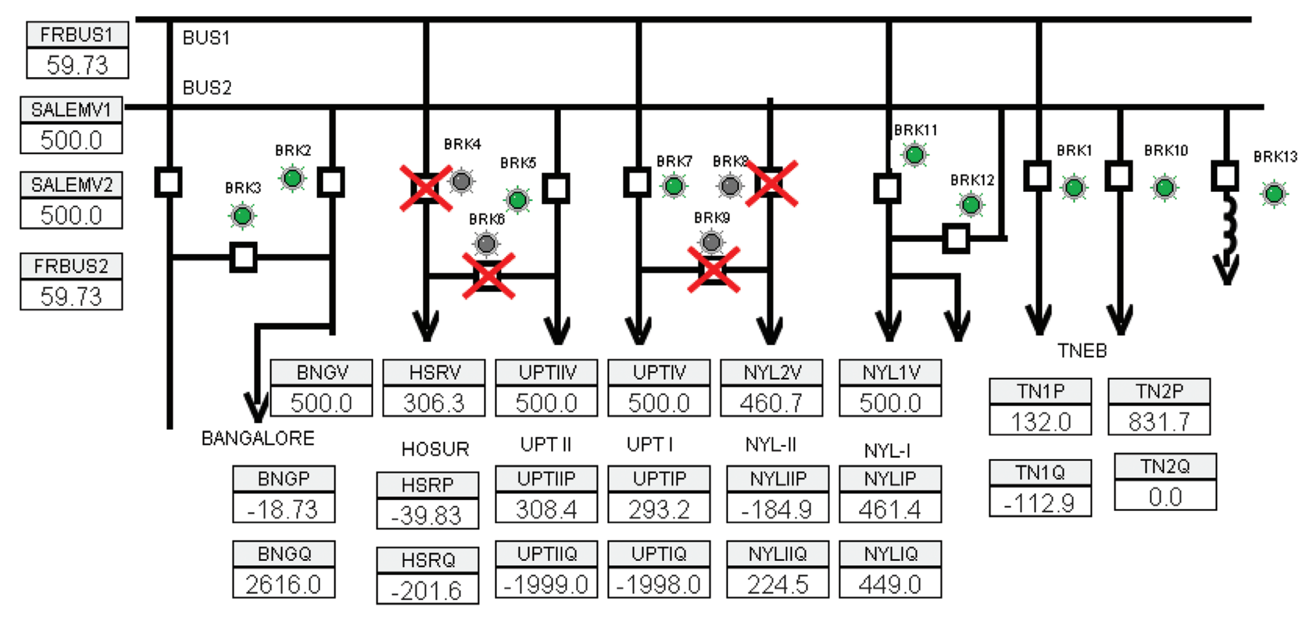

FIG. 7 SINGLE LINE DIAGRAM AND POWERFLOWS FORATTACK1WITH INCOMING LINESNEYVELI-II & HOSUR DISCONNECTED

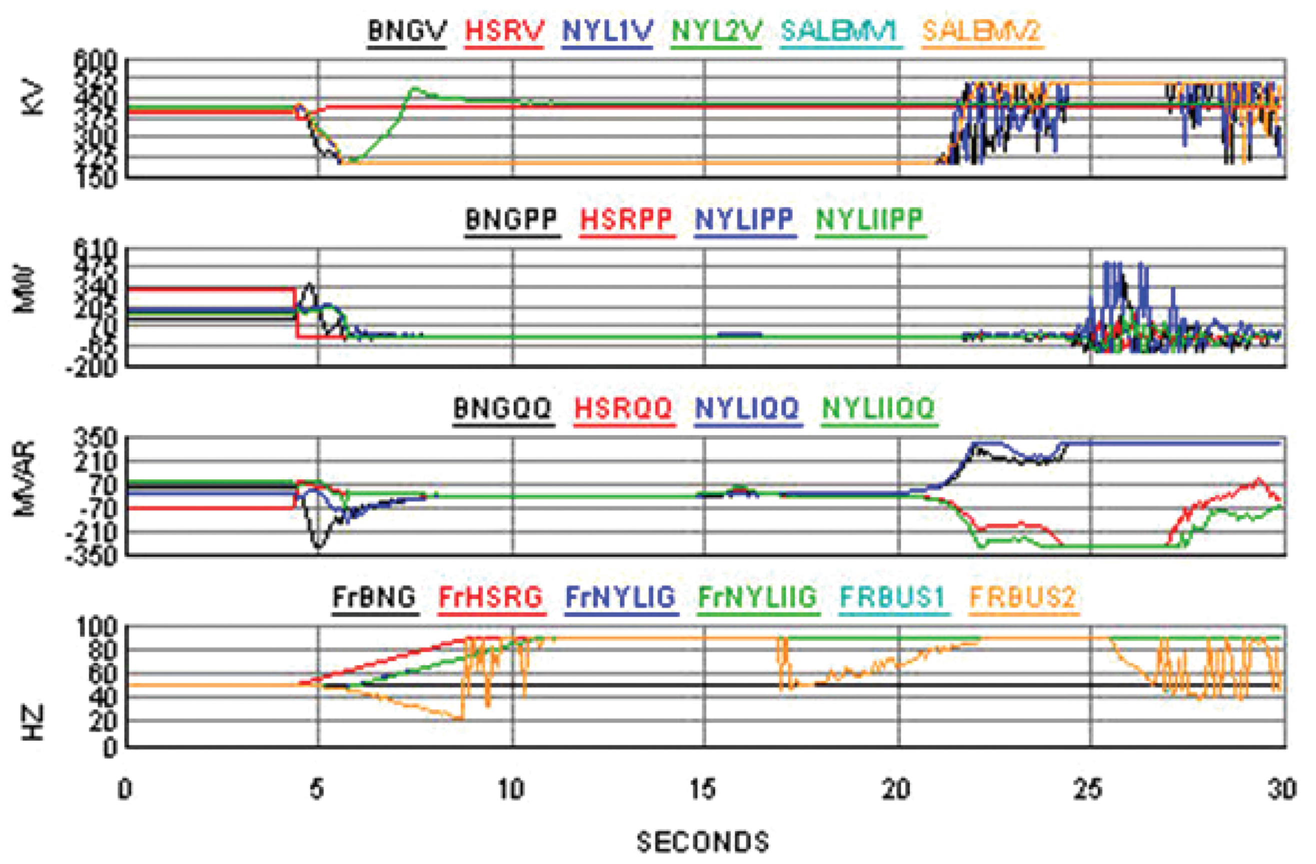

FIG. 8 ATTACK 1– VOLTAGES, P & Q FLOWS, FREQUENCYON ICOMING LINES

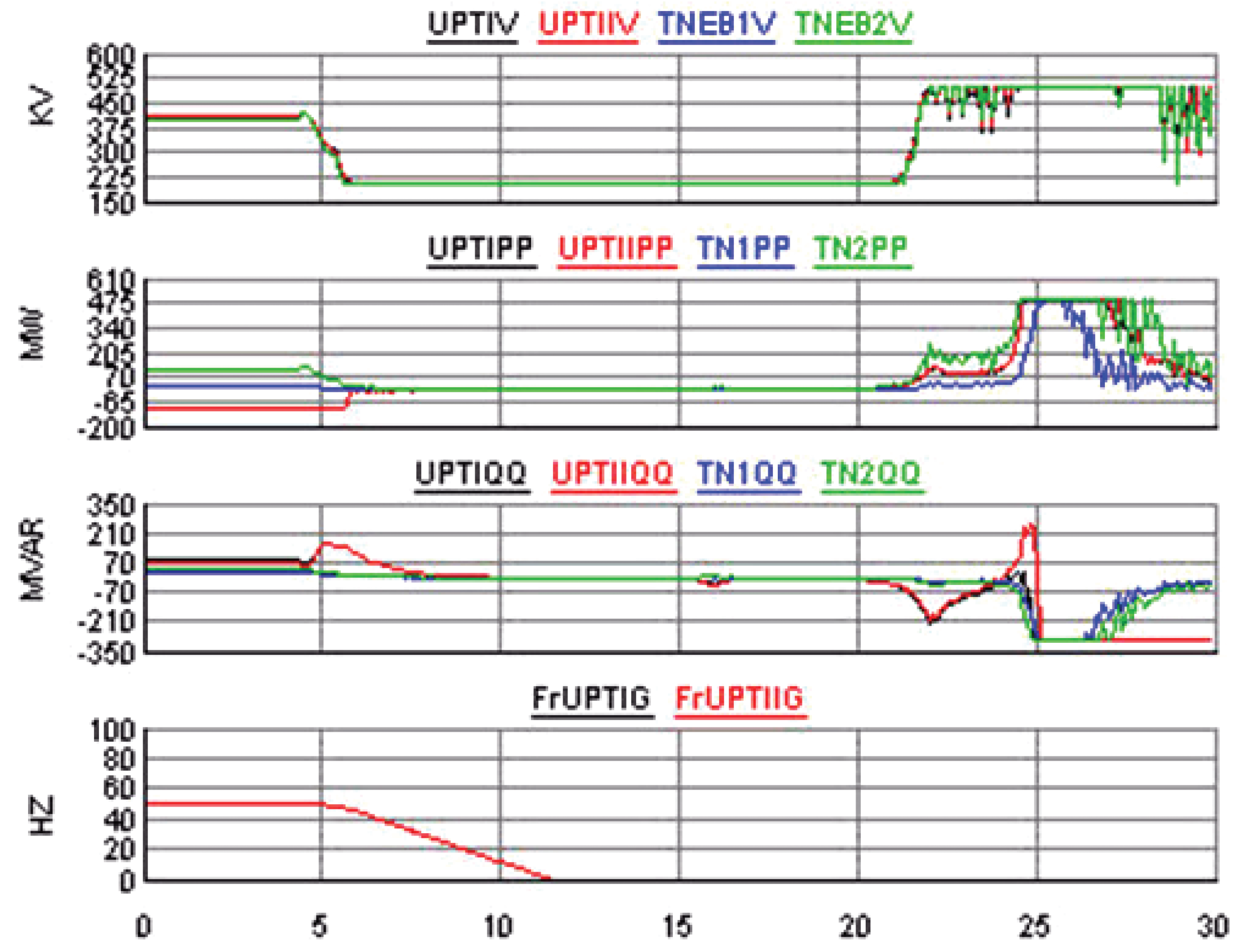

FIG. 9 ATTACK 1– VOLTAGES, P & Q FLOWS, FREQUENCYON OUTGOING LINES

B. *Tampering the generator values (Hosur & Bangalore) and Salem bus voltage and frequency by the attacker:*

In this attack, the attacker tampers the data in transit from RTU to MTU to fool the operator and force him to take unwanted action.

Healthy system data (steady state data):

Hosur:
Source MW: 319 MW, Breaker: ON
Tie-Breaker: ON, Bus voltage: 396.9kV
Frequency: 50.0Hz

Bangalore:
Source MW: 145.1 MW, Breaker: ON
Tie-Breaker: ON, Bus voltage: 400.1kV
Frequency: 50.0Hz

Salem BUS1:
Voltage: 402.1kV, Frequency: 50HZ

Salem BUS2:
Voltage: 402.1kV, Frequency: 50HZ

In this case, the Hosur, Bangalore power flows and Salem bus voltages and frequency are tampered (data modification) by the attacker. The data packet from the RTU on its transit to MTU through the attacker's machine gets modified. Incoming power from Hosur and Bangalore are tampered from healthy values of 319MW and 145.1 MW to unhealthy values of 150MW and 50MW respectively and sent to the operator. Also Salem BUS1 voltage and frequency are tampered from healthy values of 402.1kV and 50HZ to unhealthy values of 375kV and 48Hz respectively.

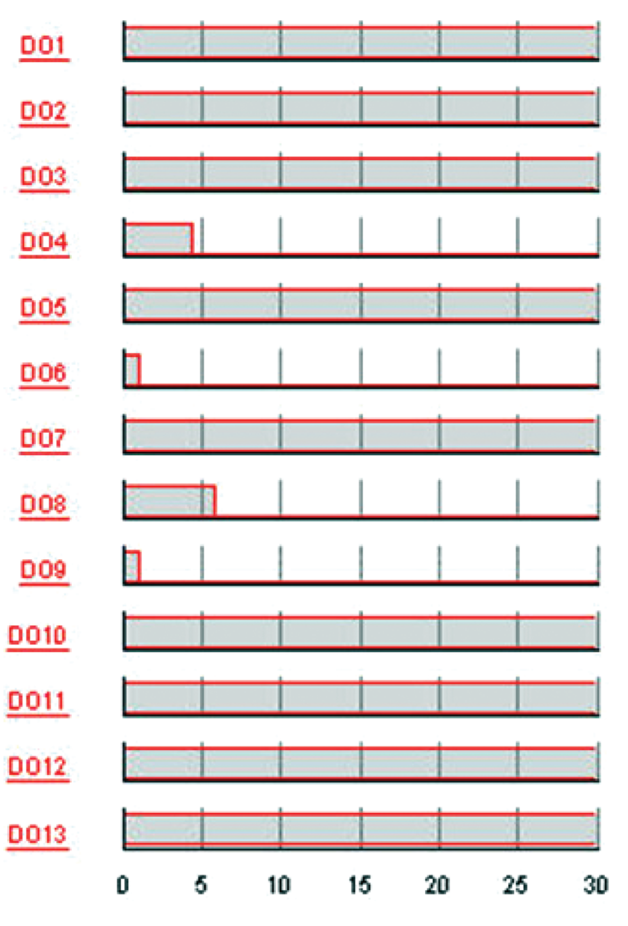

FIG. 10 ATTACK 1–BREAKER SIGNALSFROM ATTACKER

The intention behind this modification is to fool the operator into taking an unwanted action. Just modifying the incoming power values of Hosur and Bangalore cannot fool the operator into taking a corrective action as the voltage and frequency values indicate steady state. So the attacker takes extra care of modifying other dependent parameters like voltage and frequency values.This will make the operator genuinely believe what he/she is looking at. These modified values force the system operator to take corrective measure of disconnecting the Myvadi-I (UPT-I) outgoing line by opening the breakers BRK7 and BRK9 to bring back the frequency and voltage to steady state. In the realsystem, because of the loss of this outgoing line, the system becomes unstable. Single Line diagram of the system, with outgoing line to Myvadi-I disconnected, is recorded as given in Figure 11. Due to the action taken by the operator, the bus voltages and frequencies now attain abnormal values that can be seen from figures given below.

Breakers 7 and 9 signals are becoming ‘LOW’ showing the attack and all other breaker signals are ‘HIGH’. Parameters of the incoming and outgoing lines are going abnormal as can be seen from Figure 12 and Figure 13 respectively.Breaker signals from SCADA system are recorded and shown in Figure 14.

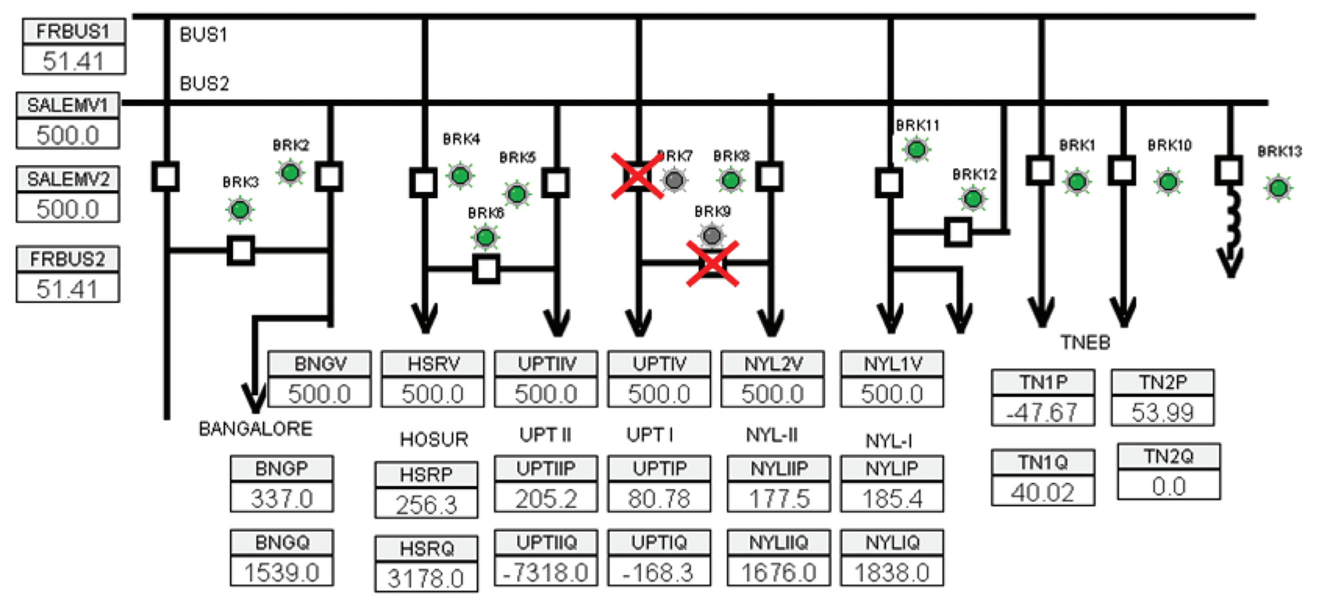

FIG. 11 SINGLE LINE DIAGRAMAND POWERFLOWSFOR ATTACK2 WITHOUTGOINGLINE UPT-IISDISCONNECTED

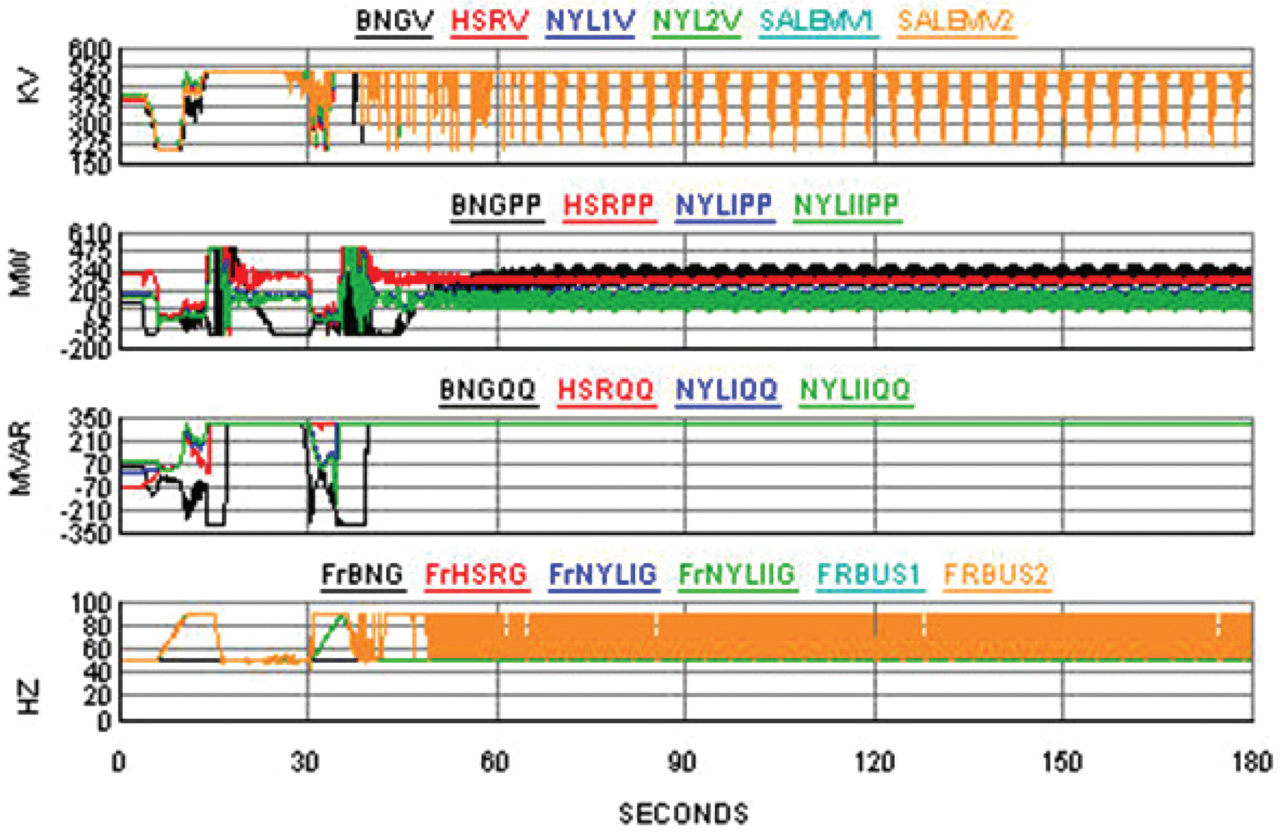

FIG. 12 ATTACK 2– VOLTAGES, P & Q FLOWS, FREQUENCYON INCOMINGLINES

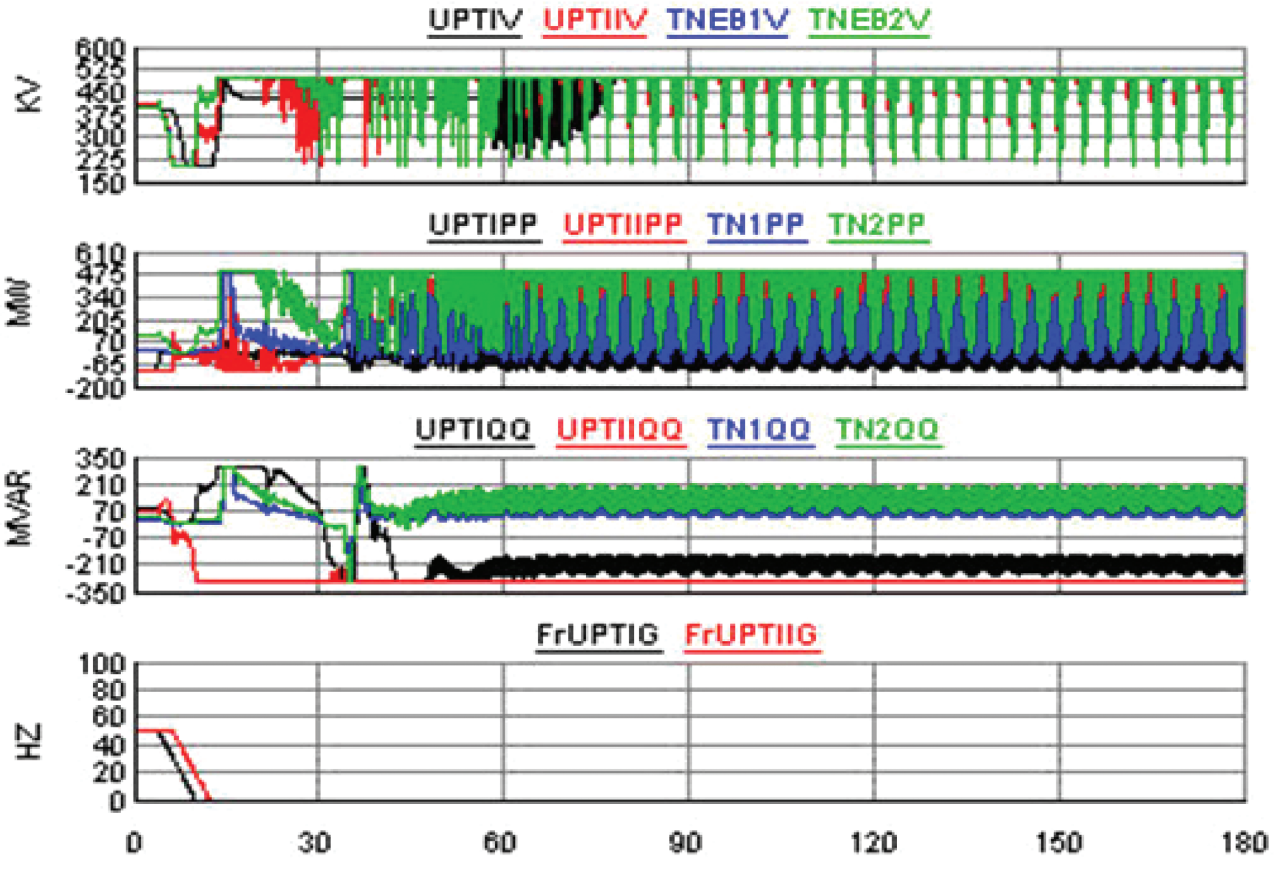

FIG. 13 ATTACK 2– VOLTAGES, P & Q FLOWS, FREQUENCYON OUTGOING LINES

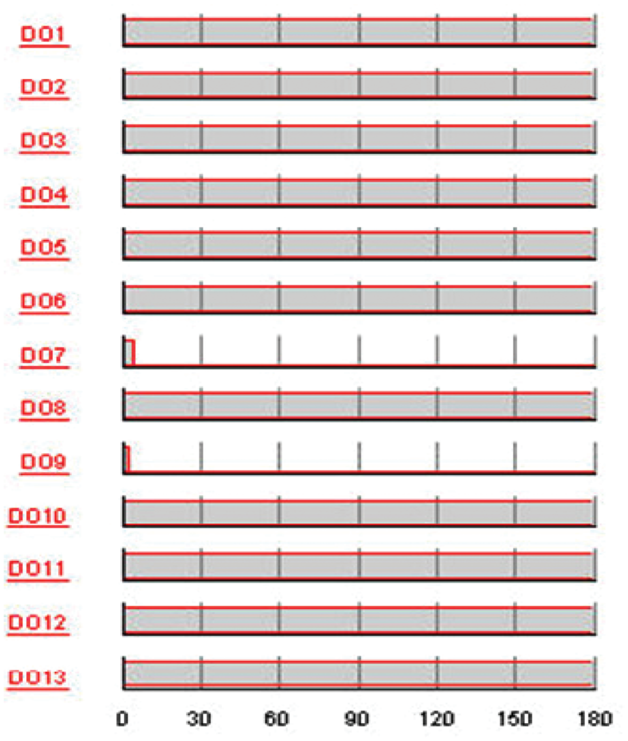

FIG. 14 ATTACK 2–BREAKER SIGNALS FROM SCADA SYSTEM

4.0 CONCLUSION

SCADA networks, like any communication networks, are vulnerable to cyber-attacks. Adoption of open protocols overcame the inter-operability problem but came with vulnerabilities as these protocols aren't designed with security in view. With the added vulnerabilities that TCP/IP networks bring, the communication in the control region of SCADA network is no more secure. Once an intruder takes control of the communication, the effect it can have is huge resulting in infrastructure loss and human loss. IEC 60870-5-101and IEC 60870-5-104 are widely used communication protocols in Transmission SCADA. Experiment to make the simulated Salem substation unstable by exploiting the vulnerabilities of IEC 60870-5-104 was conducted at CPRI, Bengaluru and the impact on the substation is recorded. The vulnerabilities of IEC 60870-5-101 have been exploited in experiments at the lab facility in C-DAC Bengaluru and similar results have been observed. So, one needs to be proactive to study the vulnerabilities and analyze the risk involved and implement appropriate security steps.

ACKNOWLEDGEMENTS

We wish to thank Smt. Sridevi J, EO, and Smt. Meera K S, JD of CPRI for their support during experiments.

We also wish to thank Shri. Raghuram, ED, Shri. S P Kumar, CM (SRC&S), Shri. Rakesh, DM, SRLDC, Bengaluru for their support and co-operation.

REFERENCES

[1] Practical SCADA for Industry by David Bailey, Edwin Wright(pages 11 -17)

[2] Soumitra K. Ghosh, "Changing Role of SCADA in Manufacturing Plan" Industry Applications Conference 31st lAS Annual Meeting, lAS '96, 1999.

[3] Practical Modern SCADA Protocols:DNP3, 60870.5 and Related Systems. By Gordon Clarke, Deon Reynders (pages 17 -35)

[4] Practical Modern SCADA Protocols:DNP3, 60870.5 and Related Systems. By Gordon Clarke, Deon Reynders (pages 46 -48)

[5] Dong-Joo Kang l, Hak-Man Kim, "Development of Test-bed and Security Devices for SCADA Communication in Electric Power System", 'Korea Electro-technology Research Institute, Incheon City College.

[6] IEC standard for IEC 60870-5-101 protocol titled "Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks".

[7] IEC standard for IEC 60870-5-104 protocol titled "Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles".

[8] Durga Samanth P, Rajesh Kalluri, Senthil Kumar R K., Bindhumadhava B.S., "SCADA Communication Protocols: Vulnerabilities, Attacks and Possible Mitigations", published in Journal, CSI

Transactions on ICT, June 2013, Volume 1, Issue 2 (pages 135-141).

[9] http://www.cert.org/information-for/denial_of_service.cfm?

[10] https://www.classle.net/content-page/connection-hijacking

[11] John T Hagen and Barry E. Mullins, "TCP veto: A novel network attack and its Application to SCADA protocols", published in Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES.

[12] IEC standard – IEC 62351-5 titled "Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives".