RESEARCH ARTICLE OPEN ACCESS

Man-In-The-Middle Attack Test-Bed in Vestigating Cyber-Security Vulner Abilities in Smart Grid Scada Systems

Kabita Manjari Samal, Tanmaya Jani,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India
Capital Engineering College, Bhubaneswar, Odisha, India

ABSTRACT
TheincreasedcomplexityandinterconnectivityofSupervisory Control and Data Acquisition (SCADA) systemsin the Smart Grid has exposed them to a wide range of cyber-security issues, and there are a multitude of potential accesspoints for cyber attackers. This paper presents a SCADA-specificcyber-securitytest-bedwhichcontainsSCADAsoftware and communication infrastructure. This test-bed isused to investigate an Address Resolution Protocol (ARP)spoofing based man-in-the-middle attack. Finally, the paperproposesafutureworkplanwhichfocusesonapplyingintrusiondetectionandpreventiontechnologytoaddresscyber-securityissues inSCADA systems.
Keywords: SmartGrid,SCADA,Cyber-security,Man-in-the-middleattack

I. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systemshavelongplayedasignificantroleinelectricalindustry,becoming increasingly complex and interconnected as state-of-the-artinformationandcommunicationtechnologiesarrive.Theincreasedcomplexityandinterconnectionhasexposed them to a wide range of cyber-security vulnerablepoints.Inpractice,maliciousattackersordisgruntledemployees may gain unauthorized access to SCADA systemsutilisingvulnerablepointsandthereafterlaunchelaborateattackswhichmayleadtocatastrophicdamages.

The IEEE Standard 1402-2000 (R2008), ‘Guide for ElectricPower Substation Physical and Electronic Security’, states:“Astheuseofcomputerequipmentwithinthesubstationenvironmentincreases,theneedforsecuritysystemstopreventelectronicintrusionsmaybecomeevenmoreimportant.”[1]

Inrecentyears,maliciouscyber-securityincidentshavehappened from time to time. For example, in July 2010, theStuxnetwormattackedtheSiemensSIMATICWinCCSCADAsystem,usingatleastfourvulnerabilitiesoftheMicrosoftWindowsoperatingsystem.Itisthemostfamousmaliciouscodeattacktohavedamagedanindustrialinfrastructuredirectly [2].

In the early history of SCADA systems it was widely believedthat such systems were secure since they were physically andelectronically isolated from other networks. Stuxnetcrossedboth the cyber and physical world by manipulating the controlsystemofthecriticalinfrastructure,demonstratingthat“securitybyobscurity”isnolongeravalidapproach.

With the development and deployment of SCADA systems,more and more cyber vulnerabilities will emerge in the SmartGrid. These vulnerabilities are not only from outside, such asterrorists, hackers, competitors or industrial espionages, butalso from utilities inside, such as ex-employees, disgruntledemployees,vendorpersonnelfortroubleshooting,siteengineers etc. In addition, cyber vulnerabilities in SCADAsystems result from deliberate attacks as well as inadvertentevents(e.g.,equipmentfailures,carelessness,andnaturaldisasters). Therefore, research on cyber-security issues for theuse of SCADA in the Smart Grid is extremely urgent andparticularly significant as one of the keynote topics in thedevelopmentofsecure systems. However,researchinthiscross-disciplinarysubjectisstillatanearlystage,andrequires much more in depth investigation and analysis ofspecific vulnerabilities. To this end, the research presented inthis paper proposes a SCADA-specific cyber-security test-bedforsimulatedcyber-attacks.Thisenvironmentprovidesaplatform for the in-depth analysis of real attack scenarios,inordertofacilitatethedevelopmentofeffectiveattackcountermeasuretoolsandtechnologiesfortheSmartGridcyberdomain.

Section II of this paper reviewsthe evolution of SCADAnetworks and their protocols in power systems. Section IIIdescribes cyber-security vulnerabilities in SCADA systemsand attack scenarios in a multilevel architecture. Section IVdiscussesrelatedworkaboutsimulation,test-bedandintrusiondetectiontechnologyforSCADAcyber-security.Section V proposes a SCADA-specific cyber-security test-bedthatinvestigatesanAddressResolutionProtocol(ARP)spoofingbasedman-in-the-middleattack.Finally,thediscussionandfutureresearchworkarepresented.

1 EvolutionofSCADAsystemsandprotocols

Tounderstandcyber-securityissuesandchallengesinSCADA systems of Smart Grids, it is better way to brieflyreviewtheevolutionofSCADAsystems.From1960stotoday,theSCADAsystemshaveundergonethreemainphasesofdevelopment,i.e.,central,distributedandnetworkedarchitecture [3].

Centralarchitecture

ThisisthefirstgenerationSCADAarchitectureinwhichmainframe systems with redundancy are in charge of all thefunctions such as Remote Terminal Unit (RTU) polling, dataprocessing,display,report,dataarchiving,andrunningapplicationprograms.ThecommunicationofSCADAisrealizedbyvendor-proprietaryequipmentandprotocol.

Distributedarchitecture

Startinginthe1980s,themajorityofSCADAsystemsadopta distributed architecture in which multiple computers in anetwork(e.g.,LocalAreaNetwork(LAN))shoulderthecomputing burden together and different computers realizedspecificfunctionsandroles.Comparingwiththefirstgeneration SCADA systems, the communication protocols aresimilar. Hence, the systems are still limited by the differentvendors.

Networkedarchitecture

ThethirdgenerationSCADAarchitectureisopensystemarchitecture, rather than a vendor proprietary environment,which utilizes open standards and protocols and distributesSCADA functionality across Wide Area Network (WAN) andnotjustLAN.Comparingwiththefirstandsecondarchitectures, the major improvement lies in the application ofWANprotocols(e.g.,theInternetProtocol(IP))forcommunication.

WiththedevelopmentofSCADAarchitecture,communication protocols in SCADA system have also beendevelopedfrompoint-to-pointlinktoopenandstandardprotocols.Fig.1illustrates abriefsurveyoftheSCADAprotocoldevelopmentfrom1970s.

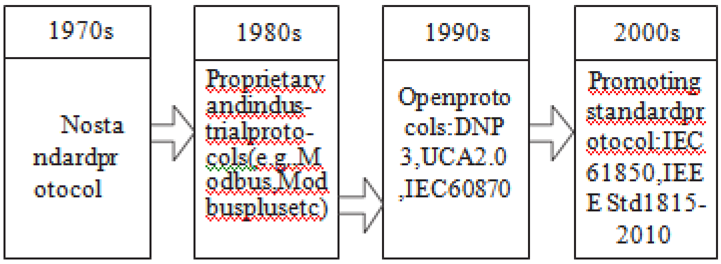

Fig.1:Thedevelopmentofcommunicationprotocolsin

proprietaryhardware,softwareandcommunicationsprotocols.However,theinteroperability,connectivity,andcompatibilityofmodernSCADAsystemsbringhugechallenges in order to make the current systems more securefrom unintentional or malicious cyber attacks. In addition,since the lifecycle of SCADA equipment is 15-20 years, it isnot uncommon that ‘smart’ and ‘dumb’ devices coexist in thefield.Therefore,itisofimportancetounderstandtheintegrationissuesbecausebothpastandfutureSCADAprotocolsarecombined in theSmartGrid.

2 CybervulnerabilitiesandattackscenariosinSmartGrid SCADAsystems

Cyber-securityinSCADAvs.ITsecurity

In current industrial and academic fields in terms of cyber-securityofcontrolsystems(e.g.,SCADA),powersystemresearchers may not master the knowledge which IT securityexpertsknow,andviceversa.Infact,therearemanydifferencesbetweenthetwoareaswhichwilldependondifferent countermeasures for cyber vulnerabilities. Table 1describes the comparison of SCADA cyber-security and ITsecurity[4].

Subject	SCADACyber-security	ITSecurity
Availability Integrity	Veryhigh	Lowto moderate
Confidentiality	Low	High
Authentication	High	Moderate
Applicationof Patching	Sloworeven impossible	Frequent
Anti-virus	Uncommon	Commonly
TechnologyLifetime	15-20years	3-5years
Timecriticality	Critical	Delaystolerated
Communicationprotocols	IEC 61850, IEC60870-5/6,DNP3, Modbusetc	TCP/IP,UDP
Computingresources	Verylimited	Unlimited
Cyberforensics	Limited,ifany	Available
Securityawareness	Poor	Good
Impactsofsecuritycompromise	Economicimpacts, equipment damageandpersonnelsafety	Economicimpacts

Table1:ComparisonofSCADAcyber-securityandITsecurity

Cybervulnerabilitiesandconsequences
AccordingtothereportoftheUSNationalInstituteofStandards and Technology (NIST) [5], there are three maincyber-security requirements for SCADA systems in the SmartGrid:availability,integrity andconfidentiality.

Anintentionalviolationofacyber-securityrequirementis
SCADAsystems
FromthehistoryofSCADAsystems,itisinterredthatSCADA systems from the 1960s to 1980s could probably besecurefromcyberattacksbecausethesystemsutilize calledanattack.Sometypicalcyberattackswhichmaycompromise SCADA systems in the Smart Grid are listed in[6], such as denial-of-service (DoS) / distributed DoS (DDoS),malicioussoftware,identityspoofing,passwordpilfering,eavesdropping,intrusion,side-channelattacks.Table2

demonstratespossiblecyberattacksandconsequencesinSCADAsystems.

Cyberattacks		Consequences	
		Cyberspace	SCADA
DoS/DDoS	Crashservices	Compromiseavailabilityand integrity;unresponsive nodes	Disable the monitoringandcontrolsystem;lossof load; loss ofinformation.
	Floodservices		
Intelligentattacks	attackprotectiverelaysetting	Compromiseintegrity	Trigger cascadingeffectswhichmayresultinamajorpoweroutage thatcanbecatastrophic.

Intrusion	IPscans Portscans	Compromiseconfidentialityandintegrity	Control aspects of thebehaviour of the systemat intruders' will whichmayleadtolosofload.
Malicioussoftware	Virus Worms Trojanhorses Logicbombs Backdoors	Compromiseavailability,integrity orconfidentiality	SCADA systems arecompromised e.g., slowdown thecommunication betweensubstations andcontrol centres.
IdentitySpoofing	man-in-the-middle message replays network spoofing	Compromiseconfidentiality,integrity	Causesafetyissuesin SCADA systems byimpersonating anauthorizeduser.
PasswordPilfering	socialengineering	Compromiseconfidentialityor accesscontrol	The severity ofconsequences dependsonthelevel ofauthority intermsofthepassword.

Table2:CyberattacksandconsequencesinSCADAsystems

CyberAttackScenarios

We propose that most cyber attack scenarios usually fall intothefollowingfive-levelarchitecture(LeverI-V).Severalattack scenarios which may cover more than one level aredescribedtoillustratehowinsidersandoutsiderscouldexploitthe vulnerabilitieslisted inthe table 2.

1) LevelI:Thetarget rangeofcyberattacksinthemostessentiallevelofthefive-levelarchitecturecontainsasubstation and field devices, such as Intelligent ElectronicDevices (IEDs), Human Machine Interface (HMI), LAN etc.Theattackpathsinthislevelcontainwiredchannels andwirelesschannels.Forexample,unauthorizedusers orattackers may access to the LAN in a substation by dial-up,Virtual Private Network (VPN) or wireless and then launchmaliciousattackssuchasportscan,sniffing,man-in-the-middleattack etc.

Scenario 1: Simulated attacks on an IEC 61850 based IED inan experimental setup is presented in [7], such as DoS attack,passwordcrackattackandARPspoofingattack. Aftersuccessful cyber attacks, an attacker can access the SubstationConfiguration Description (SCD) file including the electricdiagramofthesubstation,communicationinfrastructure,configureofIEDandIEC61850basedtraffic. Therefore,the attackermaylaunchmaliciousactionstooperatecircuit breakersbasedon identifiedinformation[8].

Scenario 2: Disgruntled employees or other attackers may beable to launch man-in-the-middle attack to sniff and interceptnetwork traffic between master station and slave station basedonMODBUSprotocolintheLANwithinasubstation.Moreover,attackerscansendfalseinformationtotheMODBUS master or slave by poisoning the MODBUS packetaddresses.Itcanbeutilizedtorealisefalseread/writecommands to the MODBUS server, block the communicationbetween the server and the client, restart the server, or evenshutdownpartofthe gridetc [9].

2) Level II: The scope of attack targets in level II covers thecontrol centre and the communication between the substationandthecontrolcentre.Thewidelyusedcommunicationprotocols are Distributed Network Protocol Version 3 (DNP3)and IEC 60870-5 serials which are lack of mature securitymechanism.

Scenario3:Anunscrupulousattackermayabletouseidentify spoofing attacks to obtain network traffic in level II.Forexample,captureddatareflectingnormaloperationsinthecontrolcentreisplayedbacktotheoperator.Itleadstothe operator's HMI to appear normal and consequently theattack will not be recognized. In addition, the attacker couldcontinue to send malicious commands from the control centretofielddevicesinlevelI,whichmaycauseundesirabledamageswhiletheoperatorremainsunawareofthe realsituationof theSCADA system[9].

3) Level III: This level mainly focuses on communicationbetweenutilitycontrolcentreswhich maybelongtotransmissionordistributionoperators,IndependentSystemOperators(ISO)orpowerplants.Themostpopularandexposed SCADA protocol in this level is Inter-control CentreCommunication Protocol (ICCP).

Scenario 4: According to the LiveData ICCP Server whitepaper[10],LiveDataICCPServercontainsakind ofvulnerability, i.e., heap-based buffer overflow. The LiveDataimplementationofRequestforComments(RFC)1006isvulnerabletoaheap-based bufferoverflow.Bysendingaparticularlycraftedpackettoavulnerable LiveDataRFC1006 implementation, an attacker may trigger the overflow toexecute malicious code or crash a LiveData ICCP Server tocauseaDoSattack.

4) Level IV: This level covers Demilitarized Zone (DMZ), anetworksegmentasa"securitybufferarea",connectingcontrolcentreswith corporatenetworks.

Scenario5:Itispossibletoestablishcommunicationconnection between corporate networks and control centres,forinstance,communicationbyTCPacknowledgementpackets.Furthermore,communicationpathssupportedbyvendors may be utilized by attackers to launch cyber attacksfromthecorporationnetworktothecontrolcentre.After

accessingtothecontrolcentre,attackersmaygainanyconfidentialandessentialinformation,modifycontrolcommands,andtampertheconfigurationfiles.

5) Level V: This level is the outermost layer in the multilevelarchitecture which includes corporate networks and connectedInternet. The cyber vulnerabilities and attack scenarios of thislevelalmost belong to ITnetwork securityarea.

Scenario 6: A utility employee who can access to computerinformation service may install or run a computer "game" orseemingly innocuous application software from a friend, ex-employee,vendororactuallyanyonewithlegitimateconnection to the employee's utility. The installed softwareincludes a Trojan horse program which opens a backdoor intothe computer network. The attacker who invents the Trojanhorseprogramcangainaccesstothecomputerinthecorporate networkfrom Internet,andfurtherlaunchmanykindsofattackssuchasDoS.Thecomputerinformationsystemsin thecorporatenetworkarenowinjeopardy[11].

Relatedwork

Increasingly,academicandindustrialrelated organisationsare focusing on cyber-security issues of SCADA systems intheSmartGrid.However,cross-disciplinaryresearchconnecting developments in power systems and IT still hassomewaytogo.Inthissection,relevantpublishedliteratureintermsofsimulation,test-bedandintrusiondetectiontechnology for SCADA cyber-security research is surveyedandsummarized.

Simulationandtest-bed

It is indispensable to set up a simulation platform or test-bedfor research on SCADA cyber-security in the Smart Grid,especially for cyber vulnerability and risk assessment, andinteraction and interdependence between power system andcyber infrastructure [6]. Moreover, there is a lack of practical,statistical and historical data about cyber-security toward theelectricinfrastructure.

Oneapproachtoobtainpracticaldataistobuildacomparativelysimplesimulationwhichcanapproximatearealsituation,forexampletheUSIdahoNationalLabSCADA test-bed [12]. The paper [13] also introduces a test-bedforSCADAcyber-securityinwhichtheexperimentillustrates the vulnerability of the network client to a DDoSattackandtheabilityoffilteringto mitigate an attack.

Inaddition,theEuropean6thFrameworkProgram(FP6) project'CriticalUtilityInfrastructureResilience'(CRUTIAL)
[14] set up two test-beds for tele-control and micro-grid tocollect data statistics and evaluate malicious attacks in gridtele-operationandmicro-gridcontrolscenarios.

Furthermore, researchers from the University of Arizona inUS[9]developedatest-bedtoanalysethesecurityofSCADAcontrolsystems(TASSCA).Thetest-bedadopteda
TCP, Modbus and DNP3 protocol analyser to

detect SCADAattackanomalies,forexampleprotocolstatetransitionanalysis.

Other researchers have tried to exploit the coupled power gridcommunicationnetworksimulatorbasedonsoftwareagentsor application program interface (API) methods [15, 16] usingcommercial-off-the-shelf(COTS)simulationtools,suchasMATLAB, PSCAD/EMTDC, OpenDSS,PSSTMNETOMAC,NS2/3,OPNET,OMNET++etc.

From published work and the above examples it is known thatauthentic simulation and accurate test-beds are effective toolsforSCADAcyber-securityresearch.However,comprehensive and well-developed tools require significanteffort to fully develop but are often propriety, hence limitedopen simulation and test-bed resources are available to thewiderresearch community.

Intrusiondetectiontechnology

Before full deployment and operation, SCADA systems in theSmart Grid will inevitably contain legacy systems that cannotbeupdated,patched,orprotectedbymanytraditionalITsecuritytechniques.Withlimitedcomputingresourcesinlegacydevicesandevennosecuritydesignfor SCADAsystems,itisdifficulttoembedtraditionalcybersecuritytechniques into the Smart Grid with legacy systems. In thesesituations, a feasible approach is to deploy intrusion detectionandpreventionsystemfor SCADAsysteminSmartGrid.

Intrusion detection technology in the IT domain is relativelymature.Numerousintrusiondetectionmethodshavebeenpresented[18]andsomeofthemhavebeenappliedintoSCADA systems [19, 20]. However, research on this cross-disciplinesubjectisstill atanearly stage.

Theprimarylimitationofthecurrentintrusion detectionsystems for SCADA is a lack of adequate knowledge andexperience of SCADA applications and protocols. The USIdaho National Laboratory [19] indicates the above limitationintermsofcurrentIntrusionDetectionSystem(IDS)application to SCADA systems, and then presents the futureSCADA IDS technologies implementing signature matching,flowanalysis,anddatainconsistencydetectiontailoredparticularly for SCADA systems. However, there is lack ofexperimentalstudy.

A. Carcano et al. proposes a state-based intrusion detectionsystem for SCADA system based on Modbus/DNP3 protocols[21,22].ThepresentedIDScontainsbothtraditionalsignature-basedtechniquesandanovelstate-analysistechniqueswhichcanmonitorcriticalstatesandidentifycomplexcyber attacks.

The model-based detection is not new in traditional IDS, e.g.,specification-based intrusion detection can be seen as modelbased.[23]believesthatmodel-basedmonitoringfordetectingunknownattacksismore feasibleforSCADA systems than general enterprise networks. The paper describesthree model-based techniques for monitoring Modbus TCPnetworks, i.e., protocol-level modes, communication-pattern-baseddetectionandlearning-basedapproach.

Arule-basedintrusiondetectionsystemforanintelligentelectronic device (IED) based on IEC 61850 is realised bySnort in [7] which develops rules by using experimental databased upon simulated cyber attacks, such as denial of service(DoS) attack, password crack attack and ARP spoofing attack.However,therulesdonotrefertoIEC61850protocolanalyses. In addition, several other new approaches have beenpresented to deal with intrusion and anomaly detection, suchas a neural network based [24] and rough sets classificationalgorithm[20].

3 SCADA-specificcyber-securitytest-bedandsimulatedattacks

In this section, a clear and effective SCADA-specific cyber-security test-bed focusing on the core level of the five-levelarchitecture in Section III is presented in order to investigatecyber-security vulnerabilities in SCADA systems. The test-bedisbasedonarealgrid-connectedphotovoltaic(PV)SCADAsystemthathasbeenimplementedinapracticalenvironment.

Test-bedarchitecture

In Fig. 2, the test-bed architecture contains five computers (A-E)andaswitch.Threewindows-basedhosts(A,B,C)simulatereal-timeSCADAcommunicationinarealsubstation LAN. The host A simulates the master station orHMI where COTS SCADA supervisory control software isinstalled.ThehostBwithanotherCOTScommunicationsoftware is a protocol gateway. The two hosts A and B areconnected by a switch. IED simulator communicates with theprotocolgatewaybyIEC60870-5-103protocol.DuetoconfidentialityandsecurityconcernsthenamesoftheSCADA software, the switch and the simulated IED in thetest-bedare withheld.

The Linux-based host D is utilized to simulate an intrudedcomputer inside the LAN or any possible laptop connected tothe LAN from the outside (e.g., maintenance laptop access),which can be illegally control by an attacker. Many cyberattacks can be investigated in the test-bed such as DoS attack,ARPspoofingattack andman-in-the-middleattack.

In addition, a SCADA-specific IDS based on The InternetTraffic and Content Analysis (ITACA) will be realised in theLinux-based host E which is connected to the LAN by portmirroring.ITACA[25]isasoftwareplatformfortrafficsniffer and real-time analysis of IP network which has beendevelopedbyCentreforSecureInformationTechnologies(CSIT) in the Queen's University of Belfast. The extendableanalysistoolenablestheimplementationof plug-intoperform specifictask,e.g.,IDS.Inthe test-bed,SCADA-specific IDS will be created using a well defined C/C++ APIbasedonITACAplatform.

Vulnerabilityscan

A comprehensive vulnerability scanning program, Nessus, isused to scan potential vulnerabilities by host on the testedsystem. The master host, the protocol gateway host and theswitch are scanned by Nessus [26] and the scan results arelistedinTable3.Forexample,boththemasterandthe protocol gateway have critical vulnerabilities, i.e., MicrosoftWindowsServerMessageBlock(SMB)vulnerabilities,which may allow an attacker to execute arbitrary code orperformadenialofserviceagainstthe remotehost.

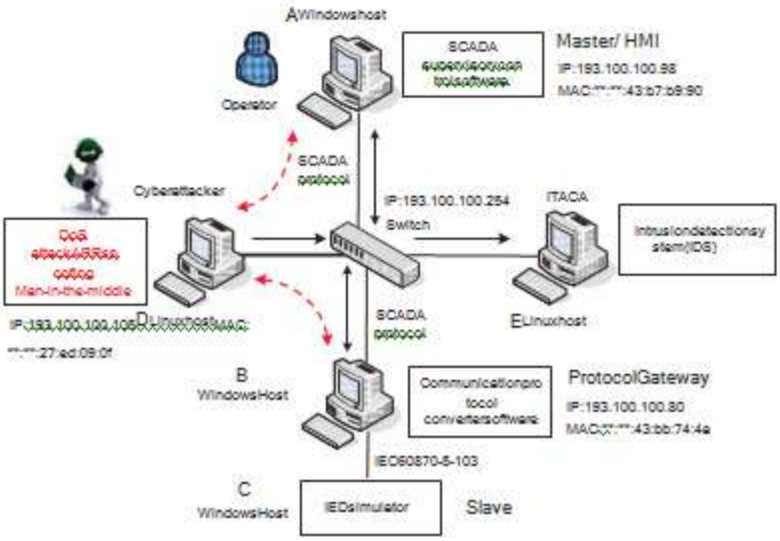

Fig.2:SCADA-specificcyber-securitytest-bedarchitecture

Host	Severity	Description
MasterWindows host *A*(193.100.100.98)	Critical(10.0)	Microsoft Windows ServerService Crafted RPC Request HandlingRemoteCodeExecution
	Critical(10.0)	Microsoft Windows SMBVulnerabilitiesRemoteCode Execution
	Medium(5.0)	MicrosoftWindowsSMBNULL SessionAuthentication
	Medium(5.0)	SMBSigningDisabled

Protocol GatewayWindows host *B*(193.100.100.80)	Critical(10.0)	Microsoft Windows Server ServiceCraftedRPCRequestHandlingRemoteCodeExecution
	Critical(10.0)	Microsoft Windows SMB VulnerabilitiesRemote CodeExecution
	Medium(5.0)	MicrosoftWindowsSMBNULL SessionAuthentication
	Medium(5.0)	SMBSigningDisabled
Switch(193.100.100.254)	Medium(6.4)	SSL Certificate Cannot Be Trusted
	Medium(6.4)	SSLSelf-SignedCertificate
	Medium(5.0)	SSLCertificateExpiry
	Medium(4.0)	SSLCertificate Signed using WeakHashingAlgorithm
	Low(2.6)	SSL / TLS Renegotiation HandshakesMiTMPlaintext DataInjection

Table3:Cybervulnerabilitiesbyhostinthetest-bed

Man-in-the-middleattackusingARPspoofing

The ARP is primarily used for resolution of network layeraddresses(IPaddresses)intodatalinklayeraddresses(Ethernet Medium Access Control (MAC) addresses) in LANcommunication. In order to obtain the MAC of a destinationhost, a source host broadcasts an ARP request to all hosts inthe LAN asking for the MAC address of the destination withIP address. The destination host responds with given IP andMACinanARPreply.Thesourcehostcachesthe<IP,MAC>pairing in local ARP cache table so that it does notneedbroadcastthe same request in thenear future.

The ARP spoofing attack is used to modify the cached <IP,MAC>pairing in the local ARP cache table. An attacker canassociate a malicious host's MAC address with IP of a targethost by modifying its ARP cache to add/update an entry withan <IP, MAC>mapping, so that the attacker can launch DoSattack, perform man-in-the-middle attack and gain access toconfidentialinformation[17].

The man-in-the-middle attack allows an attacker to sniff aLANbyARPspoofing.Firstly,theattackerredirectscommunicationtrafficbetweentwovictimhoststothemalicioushost.Then,themalicioushostwillsendthereceived or modified packets to the original destination, sothat the communication between the two victim hosts looksnormalandthevictimsmaynotnoticethattheircommunication information has being sniffed by the attacker[30]. Actually, Stuxnetcan also be described as a man-in-the-middleattackwhichfeeds monitoring software fakeinputreadings.

In the test-bed environment presented in this paper, an ARPspoofing attack is launched by a Metasploit[27] module inBacktrack 5 [28] which is Linux-based penetration testingsoftware.Alsoexaminedare,Cain,Ettercap,Seringeetc,whichareeffective toolsto launchARP poisoningattacks.

Normally,whenthe communicationprotocolgateway (IP:193.100.100.80,MAC:**:**:43:bb:74:4a)wants tosendinformation from the slave station, such as remote measurevalues, remote communication values, or collection of electricenergy,tothemasterstation(IP:193.100.100.98,MAC: **:**:43:b7:b9:90), it broadcasts an ARP request in the LAN"Who has 193.100.100.98? Tell MAC: **:**:43:bb:74:4a".All the other hosts in the LAN receive the request. However,only the host Aanswers back in an ARP reply "I have IP193.100.100.98, My MAC is **:**:43:b7:b9:90". And thenthehostB updatelocal

APRtable usingthe <193.100.100.98, **:**:43:b7:b9:90>mapping.

However,ARPisastatelessandtrustingprotocolanddoesnotprovideanyverificationmechanismtoverifytheauthenticity of the ARP requests and replies, so ARP attacksare possible launched by malicious hosts in a LAN. In theARPcachepoisoningattacklaunchedbyMetasploit,theattacker (host D) sends ARP replies to the protocolgateway(hostB)indicatingthatthematerstation(hostA)withtheIP 193.100.100.98 has the MAC **:**:27:ed:09:0fwhich is theMAC address of the attacker, so the host B will update itsARPcachetablewiththe<193.100.100.98, **:**:27:ed:09:0f>paring. The results of the APR spoofingattack are recorded in Fig. 3 by Wireshark[29]. Fig. 3 showsthattheattacker(hostD)impersonatesthemasterstation(hostA)sothattheprotocolgateway(hostB)willsendpacketsdestinedtothemasterstationtotheattackerinstead.

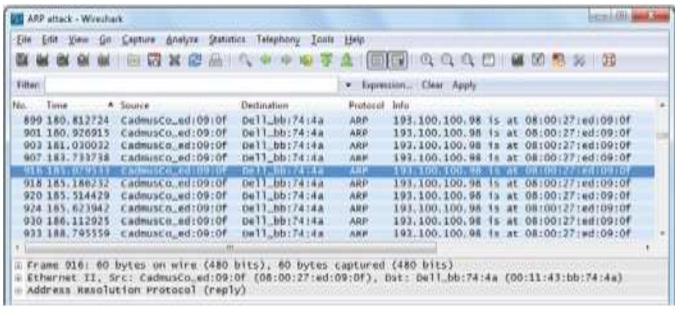

Fig. 3:The results of ARP spoofing attack on the protocolgateway(hostB) inWireshark

Similarly, the master station (host A) can also become thetarget host of ARP spoofing attack. After local ARP cache inthe master is poisoned, the <IP, MAC>pairing in the ARPcache table will be updated from <193.100.100.80, **:**:43:bb:74:4a> to <193.100.100.80, **:**:27:ed:09:0f>.Theresultcanalsobeseenfromfig.4.

Furthermore, by poisoning the master station (host A) and theprotocol gateway (host B) at the same time, the attacker (hostD) can silently stay in the middle of the two hosts to launchman-in-the-middle attack in the test-bed so that the attackercan easily sniff all the traffic sent in both directions and injectnewdataintoboth.

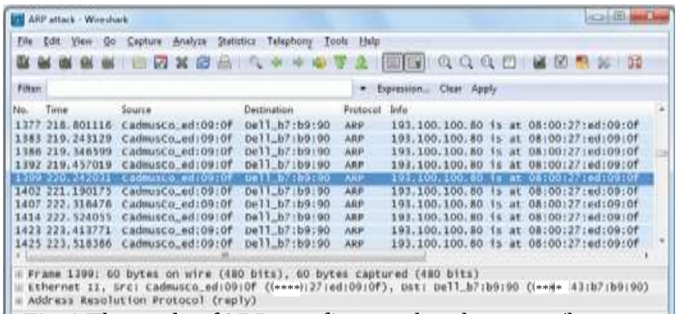

Fig.4:TheresultsofARPspoofingattackonthemaster(host A)inWireshark

Fig. 5 and Fig. 6 illustrate that the attacker can easily obtainthe communication information between the master and theprotocol gateway in the test-bed. For examples, frame 3499 inFig.5describesachangedremotemeasurevaluefrom theIED to the master, and frame 1967 in Fig. 6 shows a remoteoperation command from the master to the protocol gatewayin the SCADA system. The malicious attacker may utilize theinterceptedinformationtolaunchmoreseverattackslater.

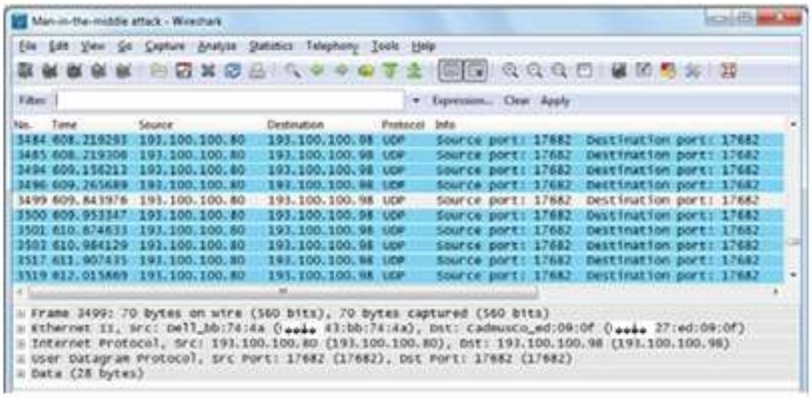

Fig. 5: The sniffed traffic from the protocol gateway (host B)to the master (host A) captured by Wiresharkin the attacker(hostD)

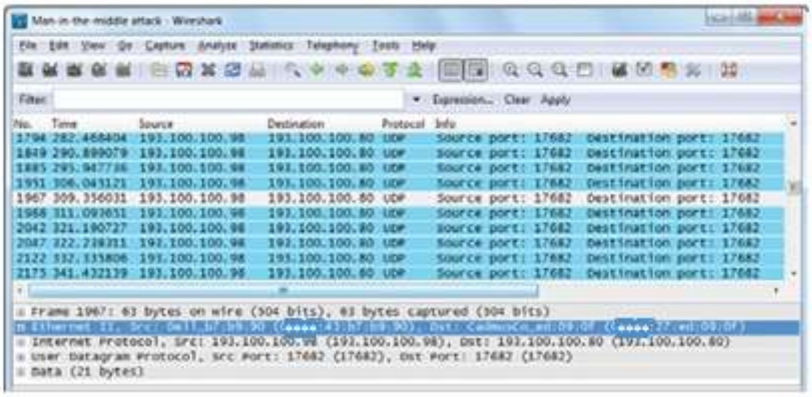

Fig. 6: The sniffed traffic from the master (host A) to theprotocolgateway(hostB)capturedbyWiresharkintheattacker (hostD)

II. DISCUSSION AND FUTUREWORK

Intheman-in-the-middleattackexperiment,anattacksimulator is developed by C/C++ programming whichcansendmodifiedinformationsuchasremoteoperationcommands,remotemeasurevaluesandremotecommunication values to the master station or the protocolgateway. The injected malicious data from the attacker willdisplay on the screen of the master host which may misleadtheoperator’sjudgement.Evenworse,thefalse remoteoperation command such as “open the circuit breaker” fromthe attacker will make the PV grid lose loads and decreasepowersupplyreliability,andeventhreatpersonalsafety.

The above ARP spoofing based man-in-the-middle attack inthe test-bed belongs to the level I of five-level architecture inSection III. The indicator of the presence of ARP poisoningbased man-in-the-middle attack can be detected by in-depthpacket analysis (e.g., IDS), because packets sniffed by theattacker have unmatched the <IP, MAC>pairing. Actually,SCADA-specific IDS can address not only known man-in-the-middleattackinthetest-bedbutalsounknowncyberattacks.

According to the aforementioned survey, investigation anddiscussion,authors’nextresearchplanistodevelop aSCADA-specificIDSagainstbothknowncyberattackssuch as man-in-the-middle attack and novel cyber attacks in theSmartGrid environment.

III. CONCLUSION

According to the evolution of SCADA systems and cybervulnerabilitiesandattacksscenariosinpublishedliterature,itis clear that a large number of potential cyber-security issuesare increasingly probable on SCADA systems in the SmartGrid. This paper provides an overview of the cyber-securityvulnerabilities of SCADA systems in Smart Grid. The paperhas also proposes a SCADA-specific cyber-security test-bedthat investigates an ARP poisoning based man-in-the-middleattack.Fromtheexperimentresults,itisinferred thatmaliciouscyberattackssuchasman-in-the-middlecaninfluence and compromise secure and reliable operation ofSCADAsystems.Therefore,researchoncyber-securityvulnerabilities for SCADA in the Smart Grid is extremelyurgentandparticularlysignificantasoneofthekeynotetopicsinthedevelopmentofsecuresystems.Finally,thepaperpresentsthatSCADA-specificIDSisapromisingapproach to address cyber vulnerabilities in SCADA systemsinauthors' futureresearch work.

REFERENCES

[1] IEEE Guide for Electric Power Substation Physical andElectronicSecurity,IEEEStd1402-2000(R2008),(2008).

[2] AntiyCERT.ReportontheWormStuxnet'sAttack.AntiyCorp.,Harbin,China.[Online].Available:http://www.antiy.net/en/analysts/Report_On_the_Attacking_of_Worm_Struxnet_by_antiy_labs.pdf,(2010).

[3] NationalCommunicationSystem,TechnicalInformationBulletin04-1:SupervisoryControlandDataAcquisition(SCADA)Systems.Arlington,VA.[Online].Available:http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf,(2004).

[4] Joseph Weiss, Protecting industrial control systems fromelectronic threats. New York: Momentum Press, pp. 29-41,(2010).

[5] TheSmartGridInteroperabilityPanel–CyberSecurityWorkingGroup.GuidelinesforSmartGridCyberSecurity.NIST,Gaithersburg,MD.[Online].Available:http://csrc.nist.gov/publications/PubsNISTIRs.html,(2010).

[6] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F.Wang,"Impactofcyber-securityissuesonSmartGrid,"in Proc. 2nd IEEE/PES International Conf. and Exhibit.on Innovative Smart Grid Technologies (ISGT Europe),pp.1-7,(2011).

[7] U.K.Premaratne,J.Samarabandu,T.S.Sidhu,R.Beresh,andT.Jian-Cheng,"AnIntrusionDetectionSystemforIEC61850AutomatedSubstations,"IEEETrans.PowerDelivery,vol.25,pp.2376-2383,(2010).

[8] C. W. Ten, J. Hong, and C. C. Liu, "Anomaly Detectionfor Cybersecurity of the Substations," IEEE Trans. SmartGrid,vol.PP,pp.1-1,(2011).

[9] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S.Hariri,"AtestbedforanalyzingsecurityofSCADAcontrolsystems(TASSCS),"inProc.IEEE/PESInnovativeSmartGridTechnologies(ISGT),pp.1-7,(2011).

[10] US-CERT.VulnerabilityNoteVU#190617:LiveDataICCPServerheapbufferoverflowvulnerability,Washington, DC. [Online]. Available:http://www.kb.cert.org/vuls/id/190617,(2008).

[11] P. Oman, E. Schweitzer, and J. Roberts, "SafeguardingIEDs,substations,andSCADAsystemsagainstelectronic intrusions," in Proc. Western Power DeliveryAutomationConf., pp.9-12,(2001).

[12] W. Dong, L. Yan, M. Jafari, P. Skare, and K. Rohde, "AnintegratedsecuritysystemofprotectingSmartGridagainst cyber attacks," in Proc. Innovative Smart GridTechnologies(ISGT), pp.1-7, (2010).

[13] C.M.Davis,J.E.Tate,H.Okhravi,C.Grier,T.J. Overbye, and D. Nicol, "SCADA Cyber Security TestbedDevelopment,"inProc.38thNorthAmericanPowerSymposium,pp.483-488,(2006).

[14] G. Dondossola, G. Garrone, J. Szanto, G. Deconinck, T.Loix, and H. Beitollahi, "ICT resilience of power controlsystems:experimentalresultsfromtheCRUTIALtestbeds,"inProc.IEEE/IFIPInternationalConf.onDependableSystems&Networks, pp.554-559,(2009).

[15] T. Godfrey, S. Mullen, D. W. Griffith, N. Golmie, R. C.Dugan,andC.Rodine,"ModelingSmartGrid Applications with Co-Simulation," in Proc. First IEEEInternational Conf. on Smart Grid Communication, pp.291-296,(2010).

[16] K.Hopkinson,X.Wang,R.Giovanini,J.Thorp, K.Birman, and D. Coury, "EPOCHS: a platform for agent-based electric power and communication simulation builtfromcommercialoff-the-shelfcomponents,"IEEETrans.PowerSystems,vol.21,pp.548-558,(2006).

[17] C.L.AbadandR.I.Bonilla,"AnAnalysisontheSchemesforDetectingandPreventingARPCachePoisoning Attacks," in Proc. 27th International Conf. onDistributedComputingSystemsWorkshops (ICDCSW'07),pp.60-60,(2007).

[18] W. L. Ali A. Ghorbani, and MahbodTavallaee, NetworkIntrusionDetectionandPrevention:conceptsandtechniques.London:Springer,pp.1-20,(2010).

[19] J.VerbaandM.Milvich,"IdahoNationalLaboratorySupervisoryControlandDataAcquisitionIntrusionDetection System (SCADA IDS)," in Proc. IEEE

Conf.onTechnologiesforHomelandSecurity,pp.469-473,(2008).

[20] M.P.Coutinho,G.Lambert-Torres,L.E.B.daSilva,H.G.Martins,H.Lazarek,andJ.C.Neto,"Anomalydetectioninpowersystemcontrolcentercriticalinfrastructures using rough classification algorithm," inProc.3rdIEEEInternationalConf.onDigitalEcosystemsandTechnologies,pp.733-738,(2009).

[21] I.N.Fovino,A.Carcano,T.DeLachezeMurel,A.Trombetta, and M. Masera, "Modbus/DNP3 State-BasedIntrusionDetectionSystem,"inProc.24thIEEEInternational Conf. on Advanced Information NetworkingandApplications(AINA),pp.729-736,(2010).

[22] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N.Fovino, and A. Trombetta, "A Multidimensional CriticalStateAnalysisforDetectingIntrusionsinSCADASystems," IEEE Trans. Industrial Informatics, vol. 7, pp.179-186,(2011).

[23] S.Cheung,B.Dutertre,M.Fong,U.Lindqvist,K.Skinner, and A. Valdes, "Using model-based intrusiondetection for SCADA networks," In Proc. the SCADASecurityScientificSymposium,pp.127–134,(2007).

[24] O. Linda, T. Vollmer, and M. Manic, "Neural NetworkbasedIntrusionDetectionSystemforcriticalinfrastructures,"inProc.InternationalJointConf.onNeuralNetworks,pp.1827-1834,(2009).

[25] J. Hurley, A. Munoz, and S. Sezer, "ITACA: Flexible,ScalableNetworkAnalysis,"IEEEInternationalConf.on Communications Industry Forum & Exhibit., Ottawa,Canada,Jun.2012(Accepted)

[26] R.Deraisonet al. The nessusproject. [Online].Available:http://www.nessus.org

[27] J. C. Foster, Metasploit Toolkit for Penetration Testing,ExploitDevelopment,andVulnerabilityResearch.SyngressPublishing, (2007).

[28] BackTrack5–PenetrationTestingDistribution.[Online].Available:http://www.backtrack-linux.org

[29] Wireshark:ANetworkProtocolAnalyzer.[Online].Available:http://www.wireshark.org

[30] Z. Trabelsi and K. Shuaib, "Man in the Middle IntrusionDetection," in Proc. IEEE Global TelecommunicationsConf.,pp.1-6,(2006).