J ElectrEngTechnol Vol. 9,No. 3:1043-1050, 2014
http://dx.doi.org/10.5370/JEET.2014.9.3.1043

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

Cyber Threat and a Mitigation Method for the Power Systems in the Smart Grid

Myongsoo Kim†, Younghyun Kim* and Kyungseok Jeon*

Abstract–Obsolescent control systems for power systems are evolving into intelligent systems and connecting with smart devices to give intelligence to the power systems. As networks of the control system are growing, vulnerability is also increasing. The communication network of distribution areas in the power system connects closely to vulnerable environments. Many cyber-attacks have been founded in the power system, and they could be more critical as the power system becomes more intelligent. From these environment, new communication network architecture and mitigation method against cyber-attacks are needed. Availability and Fault Tree analysis used to show that the proposed system enhances performance of current control systems.

Keywords:Cyber attack, Smart grid, Network architecture, Availability, Fault tree, Self-healing, Isolation

1. Introduction

A power system is a complicated interconnection system and can be categorized by power generation, transmission, substation and distribution, and a myriad of devices which should be controlled at each area. Fig. 1 shows the control systems corresponding to the power systems [1].

The Energy Management System (EMS) controls and monitors bulk power plants and high-voltage substations. The regional control centers (RCC or SCADA), controls and monitors medium-voltage substations. The small control centers (SCC) connect with unmanned medium-voltage substations. Each control system connects with each other. EMS sends control data to RCCs and RCCs send status data to EMS to estimate states of power systems. The Distribution Automation System (DAS) independently operates automation switches in distribution areas. However, DAS must connect with EMS due to Distributed Energy Resources (DER) such as Distributed Generators (DG) in the Smart Grid environment.

The power system at present must adjust to increasing demand and complexity in a changing pattern of electric consumption because electricity cannot be stored. Thus control systems are needed to dynamically generate and deliver electricity in real time manner.

In this paper, independent and hierarchical communication network architecture for Smart Grid is designed by information hiding and suppressing data exchange. The function of self-healing and resist attack will be easily implemented by this proposed network. Communication bandwidth and topology is considered corresponding to the advent of Distribution Energy Resources. Availability is also considered when it comes to design a communication network for power systems because power systems should provide seamless service. New network architecture of optical network is also proposed for the distribution area in power systems to increase reliability. Additionally, a mitigation operation algorithm using device-level intelligence is suggested if servers are compromised by cyber-attacks.

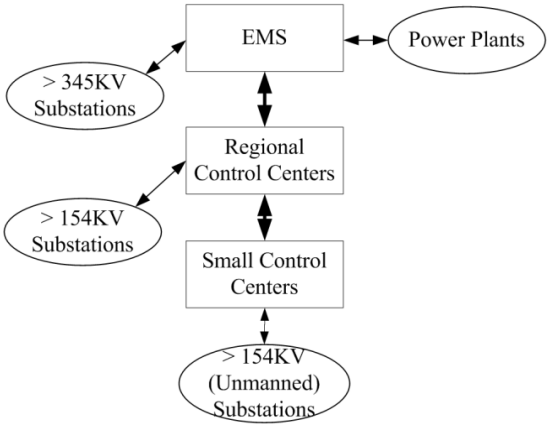

Fig. 1. The control systems and their connections between generation and substation

2. Cyber Threats in Power Systems

2.1 Cyber Attack matrix in power systems

The electrical power system is an important infrastructure which provides basic needs of life, so it has always been a high priority target for military and insurgents. Nowadays, cyber-attacks are common threats, so power systems can be attacked by cyber-attacks with or without

† Corresponding Author:Distribution Lab., Korea Electric Power Co. Research Institute, Korea. (myongsookim@kepco.co.kr)
* Distribution Lab., Korea Electric Power Co. Research Institute, Korea. ({04100212, jeonks}@kepco.co.kr)
Received: August 8, 2013 ; Accepted: December 30, 2013

physical actions [2]. The Smart Grid has introduced Distributed Energy Resource (DER), and this creates a myriad of network connections to vulnerable environments. In the Smart Grid risk may increase due to increase number of connections and number of entry points [3]. Possible attackers in the power systems are terrorists, insiders and spies. Possible goals are disrupting the system and seizing control of the system [4].

A sniffing program could be installed on the targeted system so that it enters a system and provides information to attackers on the systems' configuration, connection, vulnerabilities, and operation statuses. Hackers recently intruded utility networks and installed software which could disrupt the system [5]. Detecting sniffing attack is almost impossible unless the attacker begins injecting data to probe the configuration.

State Estimation is used in the power system to evaluate current state and predict future states of the power grid by measuring data from many sensors which are scattered in the power grids. Accuracy of measuring data is critical because estimation only depends on measured data. If data are forged, the state estimation also brings the wrong results which could cause unpredictable calamity. In this point of view, tampering with state estimation is one of the best ways to disrupt the power system; a false data injection attack could be the best attack to achieve this goal [6-8].

2.2 Stuxnet

The control systems are evolving based on open standard technologies to make power systems intelligent. Control systems have been thought to be safe from malwares, but the Stuxnet malware has been discovered in control systems [9]. Stuxnet is the first known malware that targets the controls at a specific industrial control system such as a power plant [10]. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming Programmable Logic Controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries. Fig. 2 illustrates the targeted system architecture.

In the Fig. 2, frequency converters are used to control the speed of another device, such as a motor in field level. For example, if the frequency is increased, the speed of the motor increases. Stuxnet communicates with at least 31 frequency converters to sabotage the target system by slowing down or speeding up the motor to different rates at different times [10, 11]. Stuxnet infects PLCs with different codes depending on the characteristics of the target system.

To analyze attack pattern of Stuxnet, attack trees are used. Attack tree method is a way of making decisions about how to improve security [12]. The main attack goal of Stuxnet is to sabotage control facilities such as power plants. To achieve this goal, Stuxnet modified I/O in target control process. For almost 17 months, Stuxnet targeted a specific Siemens centrifuge control component to moderate

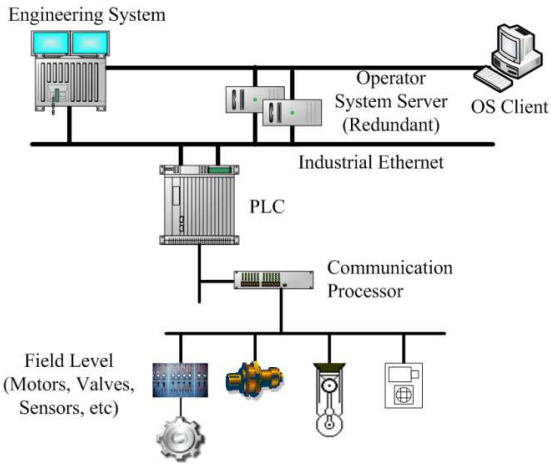

Fig. 2. The targeted system architecture by Stuxnet

the speed at which the nuclear facilities' centrifuges rotated in order to damage, but not destroy them [13].

To achieve the goal, Stuxnet used a gain in access and to create logic. The protocol used in the plant is Profibus which is an open protocol, so injection of logics is achieved by analyzing the given protocol. To gain access, Stuxnet used three sub-attacks: compromising system, getting ICS's schematics and infecting computers.

Stuxnet is designed to spread aggressively. Stuxnet used both known and previously unknown vulnerabilities to spread, and was powerful enough to evade state-of-the-practice security technologies and procedures [14]

Whenever forged software mounts on the system, the power system in the range of the device could be affected.Trojan device attack is that unauthorized outside forces can gain access to the system and can modify it or give false data to the system operators to make wrong decisions.Stuxnet is able to perform the following actions to modify PLC [14]:

- Monitor PLC blocks being written to and read from the PLC.
- Infect a PLC by inserting its own blocks and replacing or infecting existing blocks.
- Mask the fact that a PLC is infected.

Fig. 3 shows how control PC changes code block of PLC. Stuxnet is a very powerful and complicated malware, so a single solution cannot prevent an attack like Stuxnet, but a mitigation method including process and policy can significantly reduce the negative consequences that result from such an attack [15]. A proposed mitigation method will be presented in the next section.

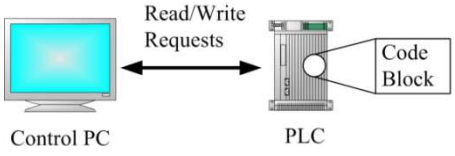

Fig. 3. Modifying PLC

3. Proposed Mitigation Method

Perfect protection of the system from cyber-attacks is not possible. Operational approaches which could mitigate the possible cyber-attacks mentioned in the previous section are proposed.

3.1 PLC and IED

In control systems, the Intelligent Electronic Device (IED) or Programmable Logic Controller (PLC) acquires the remote data, which includes meter readings, pressure, voltage, or other equipment status, then performs local control and transfers the data to the server [16].

PLCs scan their I/O by electrically reading each I/O point. This is done quickly, but in a system with lots of I/O points it can take some time to completely scan all the points. Thus, the recorded data are dependent on the scan period. If the scan period is long, some important data will not be recorded. However, IEDs have an exceptional report function, so whenever exceptional data occurs in the field, IEDs store these with a time stamp and send them to the server in real time.

PLCs are closely dependent on, and programmed and controlled by servers. PLCs are programmed by a server in a program mode and execute the program in a run mode. However an IED has its own program (firmware) and can communicate with both servers and other IEDs. We can mitigate a cyber-attack like Stuxnet by an operational method. When a server is compromised by cyber-attacks, encryption methods cannot protect remote devices from a malicious command from the compromised server. Unlike using PLC, IED cannot be modified by servers; servers just try to send control commands which make system operate incorrectly.

3.2 Device-level intelligence

The main difference of PLC and IED is intelligence. PLCs have no intelligence; only they are programmed by the server and execute the program with given inputs. However, an IED has its own program and communicates with the server; the server only sends messages to IED and IED executes the messages.

Substituting IED for PLC is one of the mitigation methods when a server is compromised by cyber-attacks. Whenever the server sends a message and if the message is the control message, IEDs check the threshold which is maximum or minimum value to protect systems from any failures. For example, Stuxnet modifies the input value of a frequency converter by 1410, but maximum value is 1210; a motor of centrifuge spins too fast and it damages the motor.

Fig.4 presents that substituting IED for PLC gives intelligent to device-level. Adding intelligence to the device-level will mitigate effects of cyber-attacks like

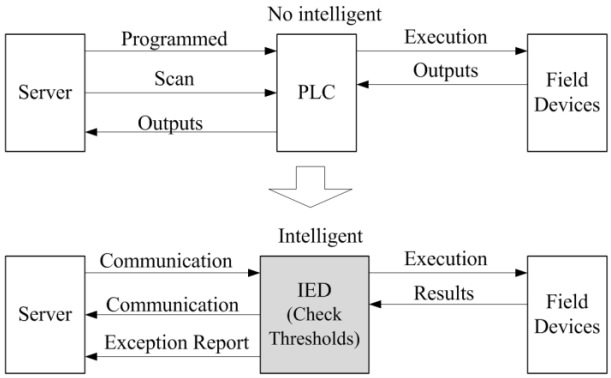

Fig. 4. Substituting IED for PLC

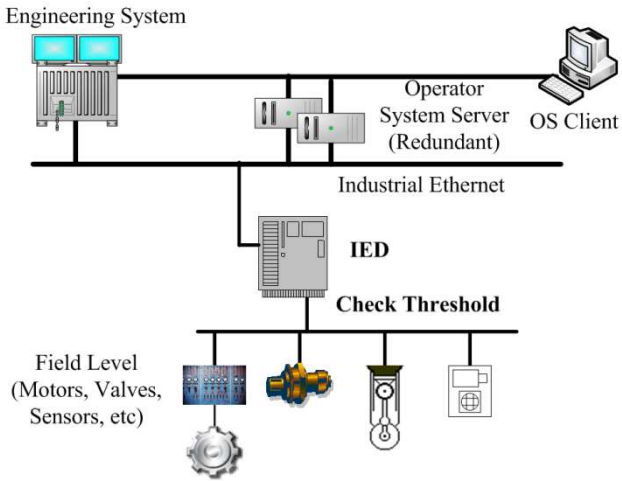

Fig. 5. Proposed system architecture in power plants

Stuxnet.

Fig. 5 shows the proposed system architecture. An IED can substitute for PLC and connect and control each field device. An IED also has communication devices, so communication processors are not needed.

Stuxnet compromised an Operator Server and made it to program a PLC to increase the speed of motors; this would cause to damage motors and the damage would spread out to the system. If an IED replaces a PLC and IED checks the increasing speed of a motor before execution, and if the increasing speed will deteriorate a motor and other systems, then IED will reject execution of the command and report a warning to other IEDs in the network.

In normal operation, a server checks status of each IED and sends commands to make a system optimal. When a server is not able to coordinate with other IEDs, each IED exchanges status with other IEDs and makes best decision to keep the systems operating correctly.

If IED decides that the command from servers is normal, IED executes the command and changes the threshold based on status of devices. If the control value exceed threshold, IED rejects the command and reports warning message to other IEDs. After then, IED goes in to autonomous operation. Autonomous operation will be

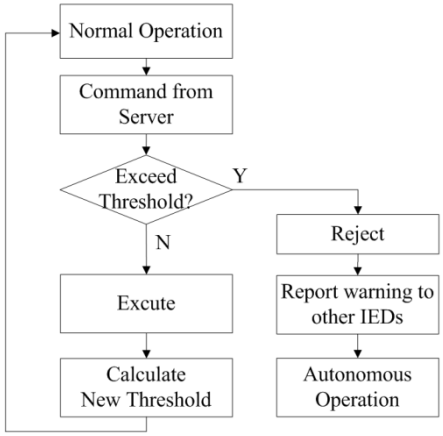

Fig. 6. Proposed defense flow chart in control systems

explained more detail in section 3.4. Fig. 6 shows the mitigation algorithm against cyber-attacks and it can be implemented as below:

Normal_operation()
IEDs receive commands from server
If the control value is exceed threshold
    reject the command;
    report warning message to other IEDs
    Autonomous_operation();
else
    execute the command;
    update thresholds;
end

3.3 Availability Analysis

Availability is one of the good tools to measure system requirements because seamless service is the important factor for power system. Availability in IEC 60870-4 is defined as below

$$\text{Availability} = (\text{MTBF} - \text{MTTR}) / \text{MTBF} \quad (1)$$

where MTBF is Mean Time Between Failures and MTTR is Mean Time To detect and Repair a failure; MTTR is assumed as 1 hour for devices and 24 hours for cable disconnection in this example.

Fault tree analysis is used to measure availability of the system [18]. Fault trees are useful to predict the overall system unavailability. From (1) unavailability can be defined by as below

$$\text{Unavailability} = \text{MTTR} / \text{MTBF} \quad (2)$$

Fig. 7 shows an example of a legacy SCADA communication system. EMS connects with distribution server by T1 or E1 line and Distribution server connects with IED by various communication modems. MTBF data are used from [19]-[22]. Table 1 shows unavailability corresponding MTBF of each component. From the given MTBF data,

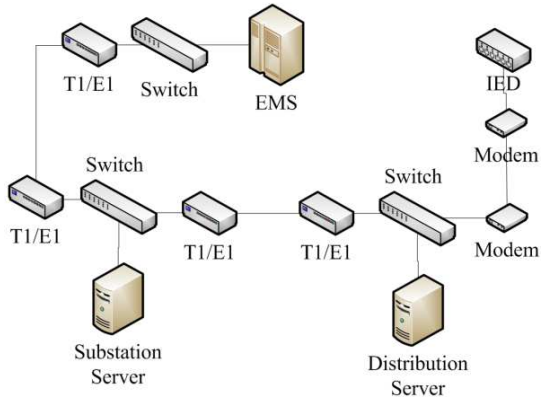

Fig. 7. Example of a legacy SCADA communication system

Table 1. Approximate component unavailability

Component	MTBF(years)	Unavailability (multiply by 10^{-6})
Server	14	8.2
PLC/IED	17	6.7
Communication processor	50	2.3
Ethernet interface	19	6
Network cable(Physical)	55	49.8

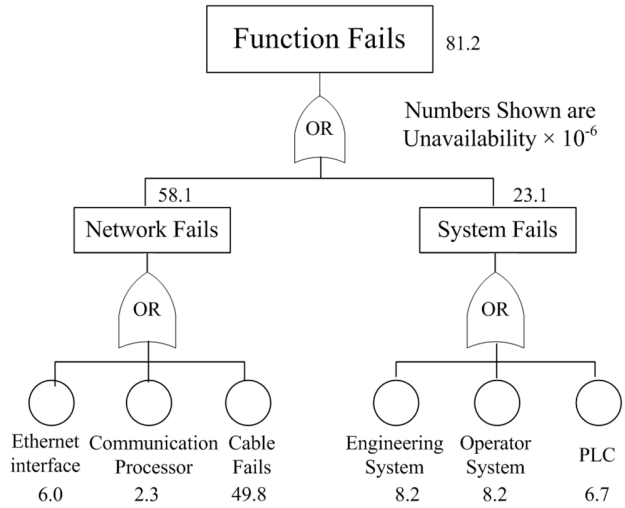

Fig. 8. Unavailability of legacy system in power plants

unavailability in Table 1 is calculated by (2). MTBF of an Ethernet switch is 20.5 years and the unavailability is:

$$\textit{Unavailability} = \left[\frac{1\ hour}{20.5\ years\ \times 365 days \times 24 hours} = 5.57 \times 10^{-6}\right]$$

The MTBF data in Table 1 are based on averaged data from fact sheets of various manufacturers, so the actual MTBF should be used to evaluate present operation components [20].

Fig. 8 shows unavailability of legacy system based on Table 1; availability is 99.9919% in normal operation

without cyber-attacks. If one of servers (engineering server or operator server) is compromised by cyber-attacks, function availability goes to zero because PLCs are dependent on servers.

Isolation and autonomous operation are applied to the legacy system to mitigate cyber-attacks. Cyber-attacks mostly affect systems not the network, so the analysis is focused on unavailability of the system not the one of the network. PLC is changed into IED and whenever IED detects cyber intrusion, IED isolates itself and does autonomous operations.

Fig. 9 shows increasing availability in field level function operation standpoints. Even if other servers fail, all field devices which are monitored and controlled by IED work correctly; IED keeps systems work properly in its boundary.Unavailability is 0.00067% with isolation of IED when servers fail due to any of reasons.

When the servers can detect cyber intrusion, function availability may be increased depending on intrusion detection rate. However, availability of legacy method reached 99.9977 in case of 100% detection rate, which is less than the result of proposed method. Fig.10 shows the simulation result.

Table 2 shows comparative function availability in field level. Device-level intelligence gives more availability to the legacy system without considering cyber-attacks. When cyber-attacks are occurred, IED must detect intrusions. Availability will be changed by the intrusion detection rate. However, most field level devices operate with limits (minimum and maximum thresholds) [3], so using threshold to detect intrusion is a proper approach.

Cyber-attacks in control systems are limited in the specific facilities, but more factors should be considered in large area and network systems. In the next section cyber-attacks will be considered in the proposed network architecture.

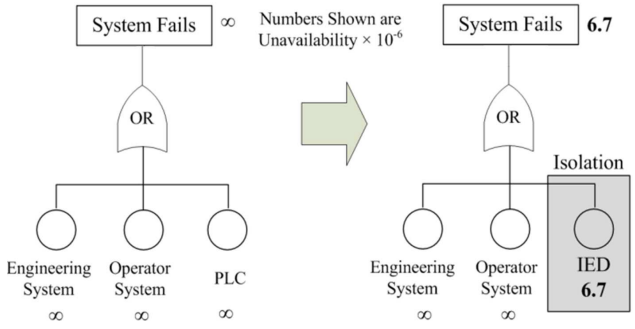

Fig. 9. Function unavailability with isolation of IED

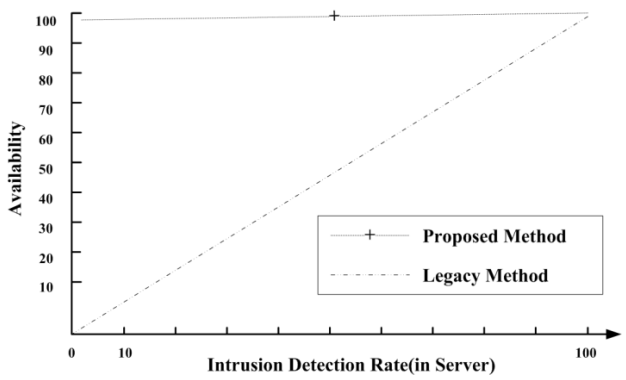

Fig. 10. Simulation result of the proposed method

3.4 Cyber defense of the proposed network

In the previous section, a mitigation method is proposed for single-site cyber-attacks. However, power control systems are connected with each other by communication networks. In this section, more detail defense mechanism will be explained based on the proposed network architecture.

In normal operation, servers (DMS : Distribution Management System) control IEDs to coordinate with other servers to make the power system optimal. Servers normally send a command of increasing or decreasing generation of electricity to IEDs.However, servers in a power system may be compromised by a malware like Stuxnet. Fig.11 shows the proposed network to mitigate cyber-attacks such as Stuxnet.

From the given network, all IEDs share their status with other IEDs in real-time manner;real-time information is the key of profitability on the Smart Grid.

If a server is compromised by cyber-attack the server sends IEDs commands which may cause disruption of power systems such as increasing or decreasing generation power. If IEDs have intelligence, they can check the validation of the command. For example, IEDs can get the

Table 2. Comparative function availability in field level

Alternative	Cyber attacks in servers	Availability (%)	Predicted annual hours out of service	Availability increasing rate (%)
Legacy system	No	99.9977	0.2	-
	Yes	0	-	-
Proposed system	Yes	99.9993	0.06	71

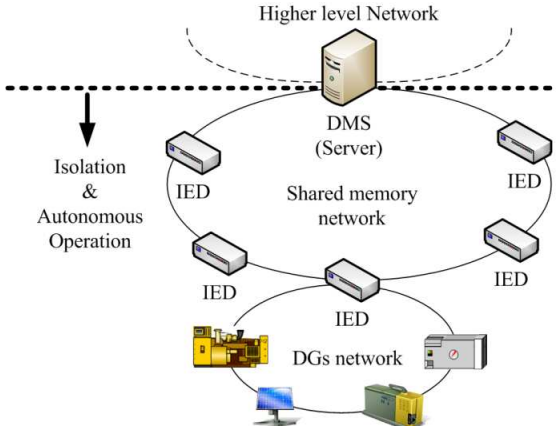

Fig. 11. Proposed network to mitigate cyber-attacks such as Stuxnet

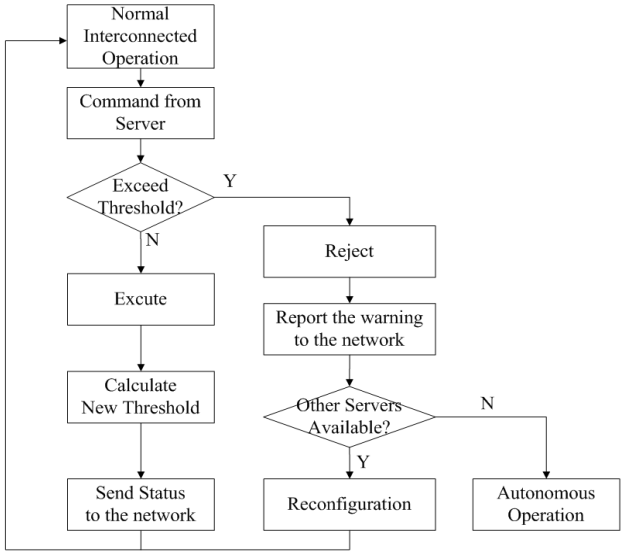

Fig. 12. Extended defense flow chart in multi-ring systems

standard frequency of electricity, 60Hz, and also can estimate the frequency of electricity after increasing or decreasing generation of electricity. If the frequency of electricity increases 4% of the standard frequency, generators start to trip and if the frequency of electricity decreases 4%, areas start blacking out [22].

To keep the frequency of electricity steady and in the bound of tolerance, EMS dynamically controls generators based on generation and demand information. Generators will be scattered in the Smart Grid, so autonomous and distributed monitoring and controlling generators is indispensable both for reliability and security. EMS makes control decision based on status of power systems, so IED has to be connected with EMS to send accurate data and receive precise control signal.

Defense flow chart in Fig. 6 may be modified for multi-ring and multi-server systems. If IEDs receive commands from a server, control value is checked by thresholds. If the result of execution with control value exceeds thresholds, IEDs reject the command from the server and report a warning message to the network. If there are available servers in the network, IEDs change network configurations and connect with the available server. If there are no available servers, IED isolates its network and does autonomous operation. This can be implemented as below:

```
Normal_interconnected_operation()
IEDs receive commands from server
If the control value is exceed threshold
reject the command;
   report a warning message to the network;
      If there are available servers
         reconfiguration;
      else
         Autonomous_operation();
      end
end
```

Fig. 12 presents this extended algorithm. When a server is compromised by cyber-attacks, the server can control all devices which connect with the server by network. However if IEDs can detect if a server is abnormal, the effect of cyber-attack will be alleviated. If an IED detects that the server is abnormal by device-level intelligence as mentioned previous section, it sends warning message to the network so that other IEDs recognize that the server is not in a normal operation mode.

When IEDs receive the warning data from the other IEDs, IEDs change its mode into 'Autonomous Operation Mode' and rejects all data and commands from the server unless the server sends 'Recover Command' with a validation method such as an one time password (OTP). The autonomous operation mode can be implemented as below:

```
Autonomous_operation()
 IEDs receive data
 If the data are sent from server
  If the data is 'recover command'
   If (Validate command)
      return normal interconnected operation mode
   else
    reject
   end
  end
  else
   update status
   if need control
      control
      send status data to the network
   end
  end
```

Fig. 13 shows the autonomous operation procedure and how to return normal operation. In Autonomous operation mode, each IED updates its status in real time manner and controls DGs to keep the power system stable. From the shared data such as total generation and availability, each IED decides which IED has higher priority to control its generator.

Other possible attacks should be considered from compromising servers. A compromised server may generate forged data and send them to the higher level server, EMS, to inject false data. If EMS receives false data, state estimation would be wrong and consequently wrong command would be sent out to the generators. Thus, IEDs should send warning message to higher level servers to protect EMS from false data injection attack.

Since IEDs connect to the higher network through a server, a compromised server can hijack a warning message if an IED tries to send a warning message to other servers. Also, IEDs only can communicate with adjacent servers, so IEDs in the network of a compromised server cannot directly communicate with EMS.

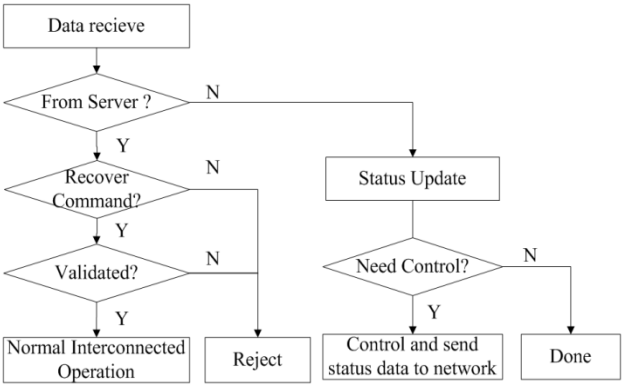

Fig. 13. Autonomous operation mode

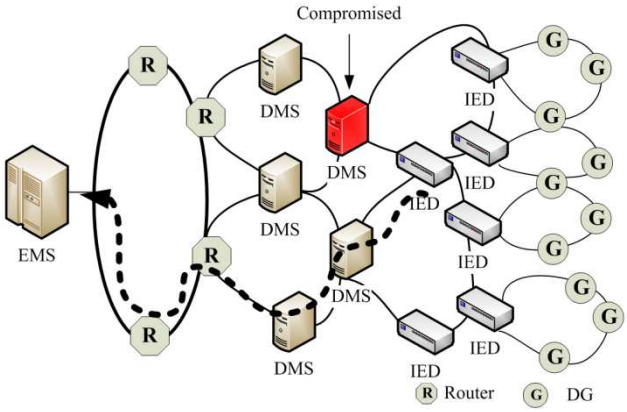

Fig. 14. Shared IED sends warning message to EMS by a detour path to prevent from false data injection attack

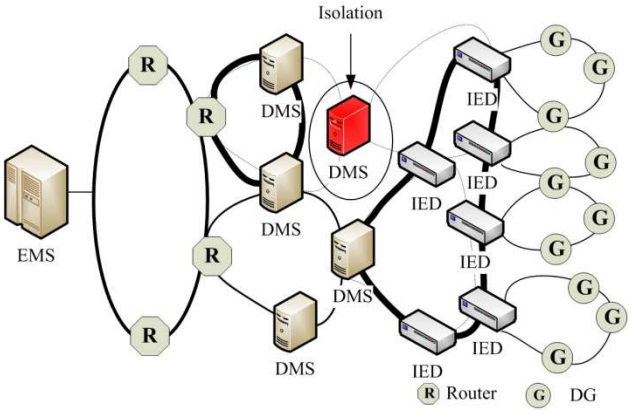

Fig. 15. Isolation of a compromised server

A proposed network in Fig. 11 can be used to solve this problem. A shared IED can send a warning message to EMS through a detour path which is not connected with a compromised server. Fig.14 shows the detour path with dashed line.

When a healthy DMS receives a warning message from IEDs, the message is forwarded EMS and other DMSs. Thus all devices in the network can know which devices

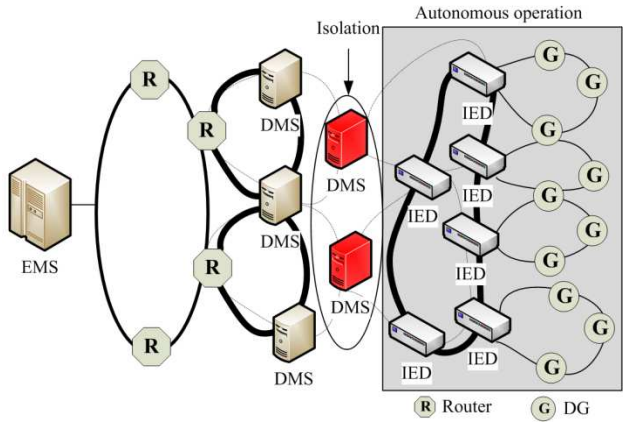

Fig. 16. Isolation and autonomous operation

are compromised. A healthy DMS takes over IEDs in compromised rings and makes a new ring network. Fig. 15 shows that a compromised server may be isolated and the other servers make a new ring network to provide seamless service.

If multiple servers are compromised and there are no available higher-level servers, IEDs operate with autonomous mode and all compromised servers are isolated. Fig. 16 shows isolation and autonomous operation in the proposed network.

4. Conclusion

Stuxnet is analyzed and a device-level intelligence operation is proposed. To minimize system impact from a cyber-attack, independent and autonomous operation is suggested. Fast isolation and self-healing functions are easily implemented by this operation mechanism.

Evolving technologies will bring lots of extra possible cyber-attacks in the power system. Thus, we need further study of mitigation methods corresponding to new cyber-attacks.

Finding optimal thresholds also can be re-studied based on field applications. Detecting cyber-attack is dependent on thresholds, so threshold update affects system reliability. More factors should be considered to calculate thresholds for other more complicated applications, such as load shedding, because this kind of application is affected by the status of other systems.

Acknowledgements

This work was supported by the Power Generation & Electricity Delivery of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government Ministry of Trade, Industry & Energy [No. 20131010501720].

References

[1] Very Large Power Grid Operators, "EMS Architectures for the 21st Century", 2005 Very Large Power Grid Operators International Working Group #2.

[2] James Andrew Lewis, "The electrical Grid as a Target for Cyber attack", Center for Strategic and International Studies, March 2010.

[3] Cyber Security Working Group, "Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements", NISTIR 7628, NIST, U.S.A., Aug., 2010.

[4] National Communications System, "Supervisory Control and Data Acquisition systems", *Technical Information Bulletin*, NCS TIB 04-1, Oct. 2004

[5] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies", *The Wall Street Journal*, Page A1, April 8, 2009.

[6] Stephen McLaughlin, Dmitry Podkuiko, Sergei Miadzvezhanka, Adam Delozier and Patrick McDaniel, "Multi-vendor Penetration Testing in the Advanced Metering Infrastructure", *Annual Computer Security Applications Conference 2010*, Dec. 2010, Austin, Texas, USA

[7] Yilin Mo, Bruno Sinopoli, "False Data Injection Attacks in Control Systems", SCS 2010 : First Workshop on Secure Control Systems, April 2010.

[8] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009.

[9] William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", New York Times, Jan., 2011, available at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[10] Symantec, "W32.Stuxnet Dossier", version 1.4, Feb 2011

[11] http://www.automation.siemens.com/mcms/process-control-systems/en/distributed-control-system-simatic-pcs-7/simatic-pcs-7-system-components/Pages/simatic-pcs-7-system-components.aspx

[12] BruceSchneier, "Attack Trees", Oct. 1999

[13] ICS-CERT, "ADVISORY ICSA-10-272-01-PRIMARY STUXNET INDICATORS", September 2010 from http://www.us-cert.gov/control_systems/pdf/ICSA-10-272-01.pdf

[14] Eric Byres, Andrew Ginster, Joel Langill, "How Stuxnet spreads-A Study of Infection Paths in Best Practice Systems", white paper ver 1.0, Feb., 2011.

[15] http://www.scadahacker.com/stuxnet-mitigation.html

[16] Motorola, "SCADA system", white paper, 2007

[17] N.H. Roberts, W.E.Vesely, D.F. Haasl and F.F. Goldberg, "Fault Tree Handbook", NUREG-0429m U.S. Nuclear Regulatory Commission, Washington, DC, 1981.

[18] G. W. Scheer, D. J. Dolezilek, "Selecting, Designing, and Installing Modern Data Networks in Electrical Substations," *Proceedings of the Ninth Annual Western Power Delivery and Automation Conference*, Spokane, WA, April 2007.

[19] M. Gugerty, R. Jenkins, and D. J. Dolezilek, "Case Study Comparison of Serial and Ethernet Digital Communications Technologies for Transfer of Relay Quantities," *in Proceedings of the 33rd Annual Western Protective Relay Conference*, Spokane, WA, October 2006.

[20] http://www.fo4all.com/t1fiberopticmodem.html

[21] http://www.scribd.com/doc/376112/Cisco-Data-Sheet

[22] http:// www.dynamicdemand.co.uk

Myongsoo Kim He received M.S. degree in Electric Engineering and Ph.D. degree in Computer Science and Engineering at Pennsylvania State University, University Park, USA, in 2008 and 2011, respectively. Since 1996, he has been a researcher of the Korea Electric Power Corporation. His special fields of interest are utility automation and communication systems in Smart Grid including utility protocol and security.

Younghyun Kim He received B.Eng. degree in information and telecommunication engineering from Korea Aerospace University (KAU), Korea, in 2002, and M.S. degree in information and communications from Gwangju Institute of Science and Technology (GIST), Korea, in 2004. Since 2004, he has been a researcher of the Korea Electric Power Corporation. His current interests are wired/wireless communication system design, analysis, and implementation in Smart Grid including utility automation.

Kyungseok Jeon He received B.E. degree in Electronic Engineering from Hanyang University and the M.S. degree in Information and Communication Engineering from Korea University, Korea, in 1986 and 2001, respectively. Since 2013, he has been a group leader of the Korea Electric Power Corporation Research Institute. His special fields of interest are communications and security in Smart Grid.