Inadvertent Threat Detection According to Power System Components

Hyuk Kim[†,††], **and Jung-Chan Na**[†,††]

[†] Information Security Engineering, UST (University of Science and Technology), Korea
[††] Cyber Security-Convergence Research Department, ETRI, Korea

Summary
Power system is exposed to security issues such as threats by external factors and multidimensional system vulnerabilities because of IT-convergence of power system. So, it is necessary to ensure availability of power system in order to keep operating. Because of application of limited security service, security capabilities of the power system can be improved through continuous monitoring of network and system as IEC 62351-7 focused on security through network and system management. Power system network structure can be divided into end system, network node and path through NSM security requirements and data objects. Component failures and network configuration changes can inadvertently result in threats like invalid network access. In this paper, we show inadvertent threats of invalid network access according to faults of components. We can categorize deliberate attack by an attacker and inadvertent threat by component failure; also it is helpful to classify the type of inadvertent threats.

Key words:
IEC 62351-7, Invalid Network Access, Inadvertent Threat, Component

1. Introduction

SCADA (Supervisory Control and Data Acquisition) system[1], which is recognized as a closed network operated independently from the external network, is being seen in a new light by infection cases of new type malware such as Stuxnet infected through removable devices. Power system is increasingly connecting with the external network for operational reasons [2]. Furthermore, as introducing Smart Grid, power system is exposed to security issues such as threats by external factors and multidimensional system vulnerabilities because power system configures IT-convergence network where it is possible to exchange information in a two-way between power providers and consumers.

Availability is one of the core principles of information security. In power system, time delay for data transmission, sensing must be strictly guaranteed to ensure availability, and it means that availability is even more important rather than integrity, confidentiality [3]. Availability is typically violated by Denial-of-Service (DoS) so that system can be paralyzed and disabled by exhausting system resources deliberately or inadvertently. It is necessary to ensure availability because disabled services, denied system access result when power system is paralyzed and disabled by DoS.

However, because security services to be operated continuously should be applied within the scope of communication delay conditions, it is very difficult to apply other security services except for access control. For this reason, security capabilities of the power system can be improved through continuous monitoring of network and system as IEC 62351-7[4] focused on security through network and system management.

According to network management functions, FCAPS (Fault, Configuration, Accounting, Performance and Security), an equipment failure causes degradation of performance so that the reliability of power system operations may be affected. Also, a change in network configuration could result in a single point of failure that is not recognized until that failure occurs.

In this paper, we focus on inadvertent threats in power system. The remainder of the paper is organized as follows: Section 2 presents the related works regarding expanded security definition on IEC 62351-7 and NSM (Network and System Management). Section 3 describes our main discussion about inadvertent threat detection by power system components. Finally, we summarize this paper and suggest the future work in section 4.

2. Related Work

IEC 62351-7 defines widely end-to-end security that encompasses not only security against deliberate attack by terrorists or cyber-hackers but also security against inadvertent threats by carelessness, equipment failure, disasters. It is to ensure security of power system operation and reliability.

Deliberate attacks are known attack like DoS, buffer overflow and so on. Known attacks are classified by existing classification methods. Previous methods of computer system attack classification are based on specific features of attack. The computer system attack can be classified by the known attack classification analysis and

Manuscript received December 5, 2012
Manuscript revised December 20, 2012

personal knowledge [5]. Features for attack classification are attack objective, effect type, ISO/OSI model level, type of the operating system, location of attack subject, type of object location, attacked service, attack concentration, feedback, attack execution initial conditions, impact type, attack automation, attack source and connection quantity. However, inadvertent threats have not been classified and defined clearly.

According to NSM security requirements defined on IEC 62351-7 for ensuring security and reliability for power system operations, NSM data object model for power system operations is defined on IEC 62351-7 in Table 1.

Table 1: IEC 62351-7 NSM Data Object Model

NSM Data Object	***Description***	***# of Object***
Communications Health	For monitoring and controlling network and protocol	61
End System Health	For monitoring and managing end system	30
Intrusion Detection	For intrusion detection	45

NSM data objects define thirteen security management requirements for network and system failure and monitoring, security intrusion detection.

3. Inadvertent Threats Detection according to Power System Components

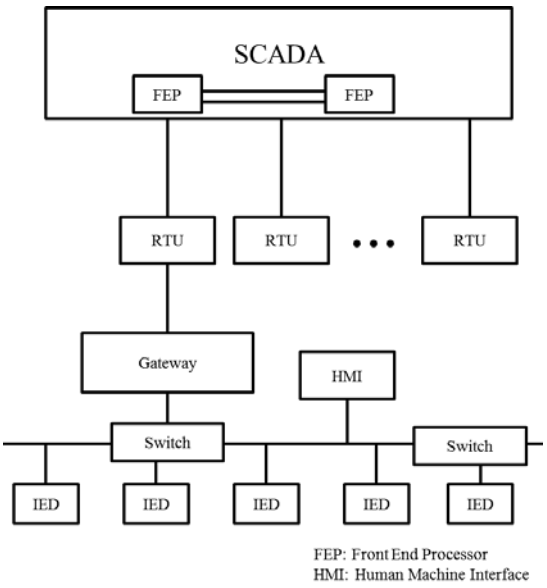

Fig. 1 Power System Network Configuration

SCADA system for power grid is made up three parts: end system, which includes Intelligent Electronic Devices (IED) and Remote Terminal Units (RTU), network node such as gateway, path like link and communication media. Figure 1 shows network configuration of the power system. Components are divided into three parts through NSM security requirements and NSM data objects. Table 2 shows part of NSM data objects for communication health that uses to monitor components.

Table 2: NSM Data Objects for Communications Health

Component	***NSM Data Object***	***Definition***
End System	*EndLst*	List of end systems connected in network
	EndDct	Detection of connect or disconnect of an end device in the network
Network Node	*NodLst*	List of intermediate network nodes
	NodDct	Detection of a new network node
	NetAltNod	List of alternate or backup network equipment for each primary equipment
	AltNodLos	Required number of alternate or backup equipment has been lost
	AltNodSw	Uncommanded switch to alternate or backup equipment has taken place
	AltNodSt	Status of network equipment
	NodLog	Log of all equipment status changes
Path	*PthLst*	List of paths in network
	PthDct	Detection of a new path
	NetAltPth	List of alternate or backup paths for each primary path in the network
	AltPthLos	Required number of alternate or backup paths has been lost
	AltPthSw	Uncommanded switch to alternate or backup path has taken place
	AltPthSt	Status of alternate paths
	PthLog	Log of all path configuration changes

According to NSM data objects, power system network structure can be divided into end system, network node and path. End system includes IED, RTU, substation masters, or any equipment with built-in computer or microprocessor processing capability. Network node includes routers, bridges, and gateways and so on. And path means something like communication links, channels or even connections.

3.1 Threat Scenarios by Component Faults

According to Table 2, NSM data objects can be divided into objects for alarm and status. Objects for alarm, such as *AltNodLos*, *AltNodSw*, *AltPthLos* and *AltPthSw*, indicate that current status is alerted when a failure occur. Others for status, such as *EndDct*, *NodDct*, *AltNodSt*, *PthDct* and *AltPthSt*, indicate current status. Through above-mentioned NSM data objects, component failures and network configuration changes can inadvertently result in threats like invalid network access.

Due to component faults or changes, the following cases occur when *TrfFrqAlm* of NSM data objects is alerted.

- Addition of end systems
- Fault or removal of network nodes
- Fault or removal of path

In case of addition of end systems in Figure 2, there are two cases that new end systems are authorized or unauthorized.

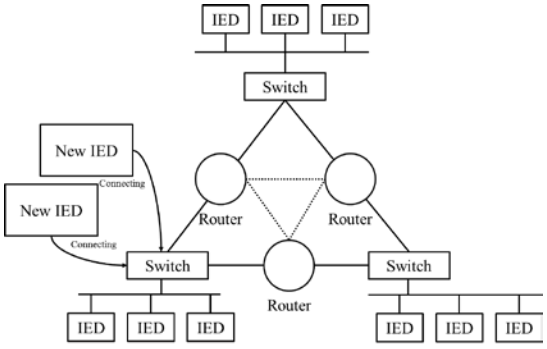

Fig. 2 Addition of end systems

First, by adding authorized end systems, network nodes like routers suffer from additional traffic generated by new things. Added end system tries to connect with other system for transfer information, and then sends request or response. So, unexpected frequency of traffic between specific systems on the network can be detected on the network node although end systems are authorized. On the other hand, in case of adding unauthorized end systems, network nodes suffer from additional traffic as well as this case may be a deliberate attack by an attacker. Attacker connects unauthorized end system for preparing attack like DoS to power system network and can generate exponential traffic into network for disabling services in power system. This case is an apparent intentional attack by terrorist, attacker and so on. In this case, we can apply for detecting anomalies using entropy difference between normal traffic and attack traffic [6].

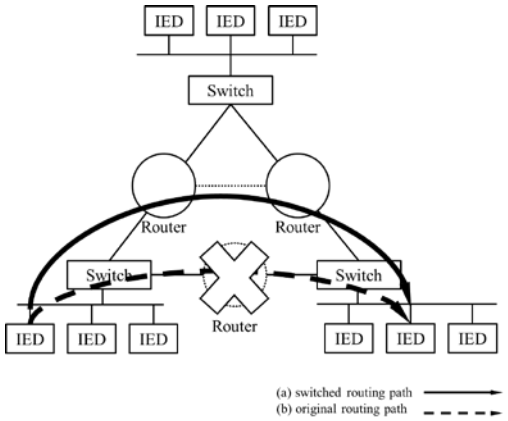

Fig. 3 Fault or removal of network nodes

Figure 3 shows how a route between systems can be changed. Originally a route between systems is (b) in Figure 3 to exchange the data between systems. When the router between systems breaks down or is removed, the route between systems is changed to (a) in Figure 3. As changing from (b) to (a), this case causes that other routers suffer from traffic between systems.

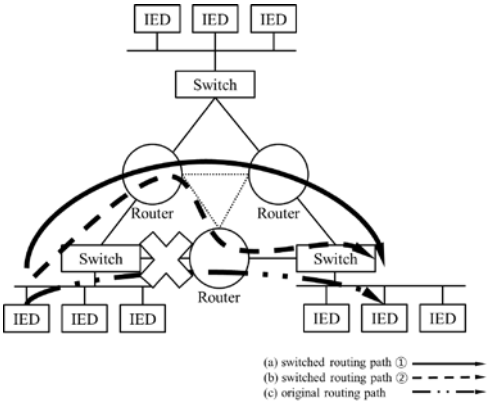

Fig. 4 Fault or removal of path

Also, unexpected traffic frequency can occur as the path to origin router breaks down or is removed. Although origin router may be passed, another router should be also passed. The traffic from source end system converges on the router, and then traffic frequency on the router will be sharply increased before *TrfFrqAlm* alert.

3.2 Inadvertent Threat Detection Process

Figure 5 shows the process that invalid network access is classified as attack according to one of components.

Once *TrfFrqAlm* occurs, we can inquire into each component to confirm their status. To inquire into end systems, *EndDct*, *TrfFrq*, *ACLLst*, *EndLst* are accessible. If connected new end system was detected by *EndDct*, we

should check current *TrfFrq* in order to decide whether new end system is generating appropriate traffic. And then, if *ACLLst* includes OID (Object IDentifier) of new end system in *EndLst*, we verify that new end system is authorized. If not, it may be unauthorized for invalid network access. In case of either network node or path, whether primary node or path changes to alternate node or path should be checked before *TrfFrqAlm* occurs so as to classify invalid network access. Finally, if it is not due to any components although *TrfFrqAlm* occurs, invalid network access is deliberate attack by attacker or excessive data request from outside.

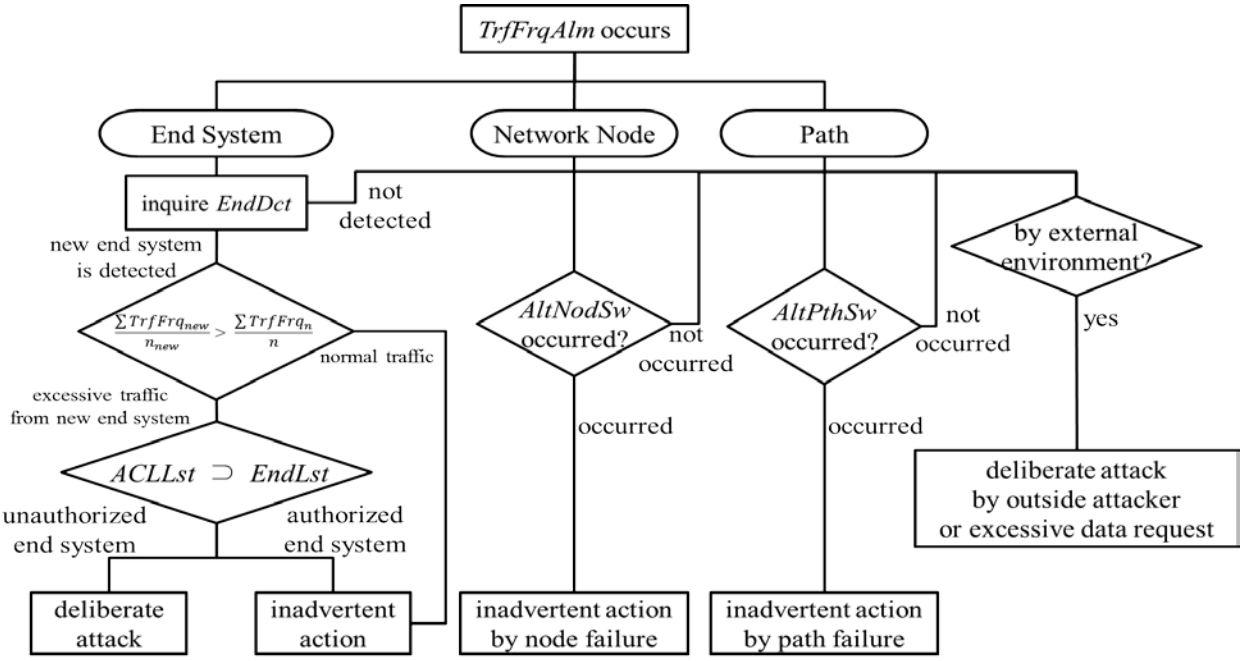

Fig. 5 Invalid Network Access Detection Flow Chart

3.2 Inadvertent Threat Detection Process

Figure 5 shows the process that invalid network access is classified as attack according to one of components.

Once *TrfFrqAlm* occurs, we can inquire into each component to confirm their status. To inquire into end systems, *EndDct*, *TrfFrq*, *ACLLst*, *EndLst* are accessible. If connected new end system was detected by *EndDct*, we should check current *TrfFrq* in order to decide whether new end system is generating appropriate traffic. And then, if *ACLLst* includes OID (Object IDentifier) of new end system in *EndLst*, we verify that new end system is authorized. If not, it may be unauthorized for invalid network access. In case of either network node or path, whether primary node or path changes to alternate node or path should be checked before *TrfFrqAlm* occurs so as to classify invalid network access. Finally, if it is not due to any components although *TrfFrqAlm* occurs, invalid network access is deliberate attack by attacker or excessive data request from outside.

4. Conclusions

As IEC 62351-7 states that end-to-end security encompasses both deliberate attacks and inadvertent actions, we should cover also inadvertent mistakes, equipment failures, software problems and natural disasters. In this paper, we suggested that it is even more important to classify inadvertent actions as well as deliberate attacks. Due to unexpected traffic frequency, we analyse related NSM data objects which include communication health and detect invalid network access after alarms like *TrfFrqAlm* occur. And then, detected invalid network access is classified in the proposed way. In conclusion, the objective of this paper is to ensure availabilities for power system operations.

However, we will work on extra studies in order to become more reliable. We will study more cases because mentioned cases of component faults or changes was highly restricted. We need to combine more and more NSM data objects and define additional NSM data objects

in order to considerably improve reliable detection and classification. Furthermore, we should experiment and evaluate traffic frequency in each case that network configuration is changed.

Acknowledgments

This work was supported by the Korea Evaluation Institute of Industrial Technology (KEIT) Grant funded by the Korea government Ministry of Knowledge Economy (No. 10041560).

References

[1] Stuart A. Boyer, SCADA: Supervisory Control and Data, 2nd Edition, Instrument Society of America, 1999.
[2] E. Byres, J. Carter, A. Elramly, and D. Hoffman, "Worlds in Collision-Ethernet and the Factory Floor," ISA 2002 Emerging Technologies Conference, Instrumentation, Systems and Automation Society, Chicago, Oct. 2000.
[3] Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, NIST, 2010.
[4] Network and system management (NSM) data object models, IEC 62351-7 TS Ed.1.0, 2009.
[5] Paulauskas, N., Garsva, E., 'Computer System Attack Classification', Electronics and Electrical Engineering, 2(66), 84-87, 2006
[6] Yu Gu, Andrew McCallum, and Don Towsley, "Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation," ACM Internet Measurement Conference, 2005.