ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 4, No.10 , July 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Anomaly Detection Mechanism based on Common NSM Data Objects for Advanced Metering Infrastructure

Seongho Ju[1], Yonghun Lim[2], Chunghyo Kim[3] and Kyungseok Jeon[4]

[1] Smart Energy Laboratory, Korea Electric Power Corporation Research Institute
Daejeon, Korea
shju1052@kepco.co.kr

[2] Smart Energy Laboratory, Korea Electric Power Corporation Research Institute
Daejeon, Korea
adsac@kepco.co.kr

[3] Smart Energy Laboratory, Korea Electric Power Corporation Research Institute
Daejeon, Korea
ch2kim@kepco.co.kr

[4] Smart Energy Laboratory, Korea Electric Power Corporation Research Institute
Daejeon, Korea
jeonks@kepco.co.kr

Abstract

The increasing role of information infrastructures in today's power system results in a demand for high level of network availability and reliability. However, unlike the traditional Information Technology environment, power system has a few characteristics, which makes us develop network and system management (NSM) data object models. The initiative steps have been launched at IEC standardization, and show what needs to be defined and monitored for enhanced reliability and availability of power system, but except Advanced Metering Infrastructure (AMI). Considering its territory and environment, it seems to be more important to develop common NSM data objects for AMI. EPRI identified a common set of AMI electric meter alarms and events later, but not NSM objects broadly. We investigate current efforts for AMI security, and then suggest the common AMI NSM objects with some exemplars in this paper. Our work is expected to become a stepping stone toward reliable Smart grid.

Keywords: *AMI, Anomaly Detection, NSM, Security*.

1. Introduction

Smart grids which are next generation of power system have become interesting nowadays. In smart grids, it is expected to control and manage energy efficiently based on advanced Information Infrastructure (IT) technologies. However, smart grids cannot help inheriting security vulnerabilities required to be solved in IT, but that is not enough. Unlike traditional IT networks which mainly focus on information confidentiality and integrity, availability is the most important factor to be met in smart grids [1]. That is the reason why Network and System Management (NSM) data object models are standardized in IEC TC57 WG15 [2], and then defined specific to AMI by EPRI Projects [3-5].

NSM data object models in [2] are defined for the purpose of the high levels of reliability as well as security in smart. They consist of 'communications health', 'end system health', and 'intrusion detection system (IDS)' NSM data object models which are divided into four, two, and seven subtopics in more details, respectively. The first model deals with network and protocol, the second one does with end system, and the last one treats intrusion detection elements to be monitored. As appears by those elements, IEC is not concerned about only security, but also all hazards including operator carelessness and equipment failure. It is reasonable to follow this type of approach for power system's availability because careless errors can cause lots of vulnerabilities in cyber infrastructure [6, 7]. It does not matter what a problem is made by, but does how a problem could be alerted to and responded by operators in a timely and appropriate way.

NSM data object models could be used to get situational awareness of power system in holistic manner by supporting communications network integrity, system and application health, and many other security management requirements [8]. However, they are specific to power system – transmission and distribution area, and won't be appropriate for AMI because of their different requirements and environments. Power system must rank availability with the highest importance, whereas

confidentiality might be the most critical problem in AMI. Most AMI components are deployed outdoor, which makes AMI more vulnerable to an act of sabotage and vandalism than power system. Contrary to power system components which provide little or no support for logging capabilities and rely on perimeter control components to detect anomalous activities, all AMI components should provide the ability to monitor, report, and/or respond against all kinds of threats regardless of their resources [3-5]. Therefore, it is more challenging to monitor and manage AMI system efficiently.

We try to define as many NMS data objects as possible from meters as well as network devices in this paper. Those objects will address electric utilities need for greater interoperability of network and security events and enable them to be better situational awareness of AMI system.

This paper is organized as follows. In section II, the latest related works are introduced. On the one hand we briefly give an overview of NSM and its relevant research outcomes, but on the other AMI security management problems are discussed with some existing solutions. This approach helps to derive common AMI NSM objects in section III, where IEC standard [2] is analyzed with some references like ANSI C12.XX in more details. The common AMI NSM data object model is verified following some use cases in section IV. We provide 'Detection-logic' based on this model to grasp the current situation of AMI system, and analyze how well the model is defined by applying a few scenarios suggested in the references [1, 3, 9]. Finally, we conclude this paper with future works in section V.

2. Related Works

2.1 Network & System Management

There AMI has been a key part of smart grid concerning about security with many interested parties [10, 11]. It is mainly because AMI handles customers' information like how much energy they are using and what the pattern of energy usage is. It is a privacy disturbance problem which could block AMI deployment in a field, and has actually happened here and there – The invasion of privacy caused by smart metering is especially the biggest concern in Europe and North America nowadays [12]. There are also other security concerns: illegally remote connection/disconnection [10, 13], energy theft [14-16], etc. To cope with these threats, it is necessary to apply authentication as well as encryption algorithms to data on the basis of appropriate key management and device authentication mechanisms. Those processes are primary security methods against threats, but not enough for the awareness of the current situation in AMI.

IEC TC57 WG15 defined what information is needed to manage the information infrastructure as reliably as the power system infrastructure [2]. The purposes of this activity are to monitor 1) network and system performance, 2) the status of device's software and hardware, 3) intrusion detection, and 4) the configuration of communications network and equipment. NSM requirements for power system operations were analyzed at first, and then NSM abstract data types and objects were defined. Those objects are expected to support communications network and system health in addition to intrusion detection. More effort into concrete NSM object model was made by mapping the NSM abstract objects to IEC 61850 [17]. However, those are all specific for the power system, but not for AMI.

Another attempt has been made to develop common AMI alarms and events for interoperability and standardization in AMI [3-5]. There are 47 security objects defined in six categories: authentication, integrity, controls, anomaly detection services, cryptographic services, and notification & signaling services. The objects are expected to contribute to a new generation of AMI SIEM (Security Information & Event Management) systems based on a consensus among the vendors. But there are two lacks as it stands now. First, they focused on only alarms and events generated by meters, but not by other AMI components such as data collectors over electric poles and maintenance service tools. Even if the meter may be the most important component in AMI, it is insufficient to have a good grip on a current state of operation based on the meter alarms and events. The second is that more objects need to be defined by analyzing the precedent studies in more details. They mainly referred to four documents: AMI system security requirements [18], security profile for AMI [19], guidelines for smart grid cyber security [20], and smart grid network system requirements specification [21]. Those documents provide security guidance with essential requirements from which common AMI alarms and events were derived. ANSI C12.XX standards were also used there, but there is substantial room for supplement which will be shown in chapter III.

2.2 AMI Security

As mentioned above, there are a few useful materials published officially as standards or guides. In [18], three categories which are primary security service, supporting security service, and assurance include 19 subtitles with

more than 500 requirements necessary to maintain a reliable system and consumer confidence. Further progress was made to provide more actionable guidance for AMI security implementation with security profiles based on some use cases [19]. The recommended cyber security controls were chosen from the DHS's ones in [22] and appropriately adapted for AMI Security. Although the guidance handles almost all the requirements required extensively, more steps should be taken to define and monitor which information is necessary to guarantee a reliable system against inadvertent mistakes and intentional attacks. It is our research work in the next chapter.

More concrete approach toward secure AMI system can be found in academic research papers which mainly deal with realistic security threats and their countermeasures. To begin with, intrusion detection for AMI is a research topic treated as an essential method for a reliable system nowadays. Berthier *et al*. [23] argue that a specification-based IDS (Intrusion Detection System) is the best approach for AMI. They suggest some detection mechanisms required to monitor AMI. For success, AMI alerts should be defined first, and then managed comprehensively to detect intrusion. The same authors work further on the specification-based IDS so as to verify its feasibility for AMI by testing its performance with realistic AMI environment [24]. In its case, of course, a kind of NSM data need to be collected and analyzed for building accurate state machines. In other words, the definition of a meaningful data object model is the first step towards a reliable AMI and smart grid.

Sometimes it is very desirable to create 'attack trees' to understand the attackers' objectives and their sequential steps because attack trees can expose to us which kinds of information would be required to effectively detect attacks. Grochocki *et al*. [9] design a set of attack trees based on three case studies: Distributed Denial of Service (DDoS) attack against the data collector, illegally remote disconnection on the meters through the data collector, and stealing customer information. The attack techniques and their targets suggested in the paper give us a hint as to the types of information required to be defined as common AMI NSM data objects. In [14], the attack tree is more specific to energy theft. The manipulation of the demand data is the final goal for energy theft with three different ways to achieve it: measurement interrupting, Stored demand tampering, and network modifying. Its contribution is the hierarchical approach which shows a number of realistic activities to the success of demand forgery. More improved attack trees are suggested in [25]. Those activities are also used for our work.

Concrete examples how to attack AMI system can be found in some precedent researches. In the viewpoint of smart grid, potential problems are categorized into five groups such as device, networking and so on, and their corresponding solutions are presented in [1]. On the other hand, attack techniques suggested in [23, 26] are more specific to AMI. However, all those scenarios show somewhat general concept, so need to be embodied enough to give us the information about how to compromise AMI and its sequential steps. In [27], a systematic method for modeling functionalities of smart meters with some attacks mounted on them. That effort is one of trials which made concrete progress and awakened our attention to security issues in AMI. Rana *et al*. studied vulnerabilities in C12.22 [28] for AMI and their usage in order to launch DoS attacks. They are concerned with DDoS attack and identify three attack scenarios that exploit vulnerabilities in ANSI C12.22 services: trace service, resolve service, and urgent traffic. The proposed solutions to those attacks which are many realities also need to gather and analyze some kinds of NSM data objects.

Apart from the security concerns, it is worth surveying the materials addressing AMI system in itself consisting of communication networks and metering-related devices. The interconnection between metering devices [28, 30] can give rise to security problems, and data table in a metering device [29] is directly related to AMI security because it is a target to be secured. We refer to the specifications for AMI components that KEPCO draw up as well [31]. The document gives in detail the functions and services which all the data concentrators and communication devices shall support as AMI components on the basis of well-defined KEPCO AMI protocol as well as IEC 62056 standards. All those things can also be useful identifying a set of common AMI NSM data objects and improving our ability in detecting and responding to any abnormal condition.

3. Common AMI NSM Data Object Model

Taking into consideration the above references, we fit NSM data objects in [2] to suit AMI, but maintain the previous frame with three subcategories: communication health, end system health, and IDS. Some NSM data objects are deleted, whereas others are newly added for AMI. We do show causes for not all the revisions, but some critical ones here because of the limited space. Then, some scenarios where newly added objects are used to catch their abnormal situations will be given for your understanding in the next chapter.

3.1 Communication Health

The previous document [2] defined 61 NSM data objects for 'communication health'. The number of redefined ones in this paper is 63: five objects are left out of, whereas seven more ones are supplemented to the result of [2]. First, 'PthLst' which means the list of paths in network is redundant as 'PthRoutLst' also contains the same information. As for 'ConnFailAlm', it can be predicted as 'ConnFailTmms' time as later after 'ConnAlm' occurs. Three others can be removed by the reasons as shown on Table I. On the other hand, there are seven objects to be added to meet the requirements of AMI. As AMI is more vulnerable due to its coverage up to Home Area Network (HAN), it is essential to monitor any control signal coming from HAN to meters and block it if detected. That is the reason why we add 'ConSigAlm' to the list. As for 'AddrResAlm' which is referred to [28] as a relay's function, it is helpful to find out where the problem is caused by in case the connectivity to any C12.22 device is lost. We also add four more objects for the same reason on the bottom of Table I.

Table 1: Communication Health NSM Data Objects for AMI

Object	Description	Revision
PthLst	Desirable to be a component of 'PthRoutLst'	Delete
ConnFailAlm	Deducible from combination of 'ConnAlm' & 'ConnFailTmms'	Delete
ConnTotTmms	Deducible from combination of 'ConnFailTot','ConnCurTmms', and(or) 'RsTmms'	Delete
ConnAvTmms	Deducible from combination of 'ConnFailTot' & 'ConnTotTmms'	Delete
ProAcsAlm	Not different from 'ProtMisAlm'	Delete
LgiFailCnt	Number of unsuccessful login	Add
ConSigAlm	Detection of control signal from HAN	Add
AddrResAlm	Address resolution service failure alarm	Add
SessToutAlm	Session timeout alarm (inactive session)	Add
ResInvAlm	Invalid response for request	Add
NegFailAlm	Negotiation request not accepted by client	Add
TermSesAlm	Terminate service invocation	Add

3.2 End System Health

Table 2: End System Health NSM Data Objects for AMI

Object	Description	Revision
FwUpgAlm	F/W upgrade failure	Add
AppUpgSt	Status of S/W upgrade	Add
AudRrdAlm	Change in audit record	Add
AudStrAlm	Audit storage exhaustion or failure	Add
AudStrMax	Maximum storage capacity for audit record	Add
AudInvAlm	Invalid or inaccessible audit record	Add
UsgDatClr	Electricity usage data deletion	Add
UsgDatTabMod	Electricity usage data table modification	Add
UsgDatLog	Change related to electricity usage data	Add
TestPrtAlm	Enabled configuration or test port	Add
SelTestAlm	Security functionality self-testing failure	Add
SessLckSet	Set session lock period (for automatic locking)	Add
AudFncSt	Status of audit function operation	Add
SecSetChgAlm	Security-related setting changes	Add
EndTampAlm	End device tampering detection	Add

Monitoring and management of end systems involve internal and external assessment of their health. The targets to be monitored are the exchanged and stored data, application or software module, and the status and operation of end systems. Fifteen objects are more defined, whereas none are removed from [2] as shown on Table II. The upgrade of firmware or software in meters is not a special order any more in AMI, so it is natural to monitor the software-related objects ('FwUpgAlm' and 'AppUpgSt'). Audit record within meters is very important enough to define 'AudRrdAlm', 'AudStrAlm', 'AudStrMax', 'AudInvAlm', and 'AudFncSt' for AMI security, just like IT networks. Electricity usage data are worth monitoring in AMI system as it is directly related to billing service. Therefore, any illegitimate access to electricity usage data shall be detected and set straight. 'TestPrtAlm' is for preventing the test port of meters from undesirable usage, and 'SessLckSet' is for automatic session locking after the management job is finished in case of illicit access through the unintentionally unclosed session. The tampering detection, response, or even evidence is required at the level of end system according to the several references (EndTampAlm).

3.3 Intrusion Detection System

Table 3: Intrusion Detection System NSM Data Objects for AMI

Object	Description	Revision
UnAuthUsrCnt	Deducible from 'UnAuthAlm'	Delete
ComLosAlm	Deducible from 'ConnAlm', 'ConnFailAlm', & 'EndDct'	Delete
ComOnAlm	Deducible from 'EndDct' & 'NodDct'	Delete
PwrLosCnt	Deducible from 'PwrLosAlm'	Delete
ComLosCnt	Deducible from 'ComLosAlm'	Delete
UnAuthOpr	Unauthorized operation	Add
InitAuthPro	Authentication process initialization	Add
AuthProAlm	Authentication process failure	Add
CodIntChkAlm	Code integrity check failure (especially when F/W is upgraded)	Add
PduIdeCnt	Number of identical data transmission	Add
UsrCurConnCnt	Number of concurrent sessions belong to the same user	Add
CertInvAlm	Invalid certificate alarm	Add
KeyInvAlm	Invalid secret (including security key) alarm	Add
CrpOprAlm	Failure related to cryptographic operation	Add
ChgAcsAlm	Change in access control or privilege	Add
ChgUsrAlm	Change in user or password	Add

In this category, we newly define eleven data objects the moment get rid of the five existing ones. The reasons for the deletion are briefly presented next to the objects, and they are understandable. We try to give more space to the added objects instead. Any operation without

authorization shall be strictly prohibited, but none of the existing objects have to do with it. 'UnAuthOpr' can be used to realize all such operation. When it comes to authentication process, 'InitAuthPro' for the process invocation and 'AuthProAlm' for its failure are defined here. The object, 'CodIntChkAlm', will be reported whenever any failure occurs during checking the integrity of transferred code. It is especially for the firmware to be downloaded into meters and then remotely upgraded. This sort of function will be useful for more flexible and intelligent services someday introduced through AMI. Both 'PduIdeCnt' and 'UsrCurConnCnt' can foreshadow upcoming attacks or accidents, and incomplete connection or communication will be expected from three invalid alarms: 'CertInvAlm', 'KeyInvAlm', and 'CrpOprAlm'. Any change in predefined access control, privilege, or password shall be double-checked its legitimacy. It may be directly linked to security accident otherwise.

AMI NSM objects defined above can be categorized in more details, but not recommended because of too many sub-objects identified to be handled. In case of 'UsgDatTabMod', for example, tens of tables each with tens of data fields are defined in [30], which addresses to monitor hundreds or even thousands of objects. Hence, it is desirable to leave the task within a private scope.

4. Verification

In this chapter, we provide the concept of 'detection-logic' first. It is the contrary concept of 'attack-tree' which is introduced by Schneier in [32], and is a basic flow based on NSM data objects in the detection of aberrant operation in AMI. Some case studies on how well common AMI data objects are defined and fit AMI system management are adduced thereafter.

4.1 Detection Logic

All the NSM data objects may not be used at the same level for the system management. Some are set, monitored, and controlled ever since the early stage of management, others are carefully watched and analyzed after any signs are detected. They also seem to correlate in keeping with regulations. We try to establish interconnection and sequential order among them in this chapter. To achieve this, we sort them into several categories first, and then identify what is required to be looked into more deeply after what is reported.

NSM data objects are classified into four groups: ordinary setting or monitoring, bellwether of abnormality, corroborating evidence, and final decision with some response. Some objects belong to more than two groups depending upon the situation.

1) Group 1 - Ordinary setting or monitoring: These objects, the class of which is 'configuration setting', 'status', or 'value', play an ordinary role in monitoring AMI system. They provide the information about the present operating situation, and enrich our recognition of characteristics specific to AMI through a process called statistical analysis. Thus, they are informative and involve valuable meaning to apprehend AMI environment, but sometimes bother AMI managers because of their frequent report and large volume: the processing and storing this data are another concern. Members of this group are 'EndLst', 'NodLst', and whatnot.

2) Group 2 - Bellwether of abnormality: Most 'alarm' objects should be included in this group. They are reported to management center whenever their preset conditions are met, and imply whatever happens as we call abnormal symptoms. Once the bellwether of any attack or system error is alerted, more objects in group 1 and/or 2 are examined deeply, and then we pick out the handful that seem to give more definite circumstantial evidence. Simple investigation is done to roughly predict a few possibilities in this stage.

3) Group 3 - Corroborating evidence: More progress should be made by finding the correlation, causal connection, and sequence among selected objects. For instance, 'ConSigAlm' on Table I might be normally followed by 'NegFailAlm', 'AuthProAlm', 'CertInvAlm', etc. It is the case that malicious intent is suspected and more evidence is required to confirm whether it is a kind of problem to be handled or not. 'Log' objects may be used as supporting evidence. An example is as shown in Fig. 1.

4) Group 4 – Final decision: The objects that divulge the actual state in themselves are returned as final judgment to a system manager. 'AtkTyp' with or without 'AtkAlm' are reported in case of attack, and 'BufOvAlm' or 'BufUnAlm' in case of buffer problem. 'UnAuthOpr' has much broader meaning with lots of preceding evidential objects. It represents an attempt at compromising devices if 'AuthProAlm', 'CertInvAlm', 'ChgAcsAlm', and the like are already reported, and an attempt at accessing network if it is followed by 'NodDct', 'UnAuthAlm', 'NetAcsAlm', and so forth. Whereas it announces network damage after 'ConnAlm', 'ConnExcAlm', or 'SynAlm' are alarmed.

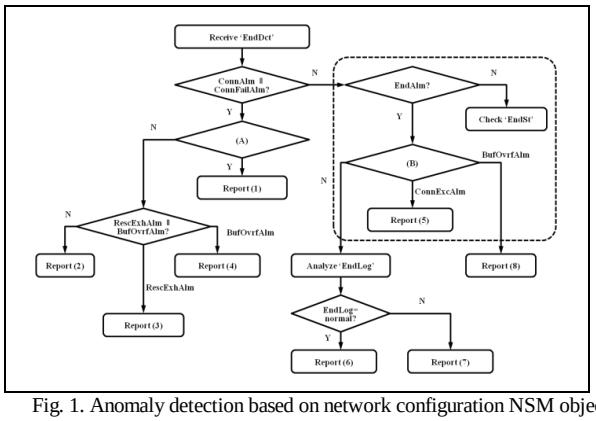

Fig. 1. Anomaly detection based on network configuration NSM objects

In explaining detection logic concept, we will use some NSM objects which we decide to remove from common AMI NSM data object model. They are ConnFailAlm, ConnTotTmms, ConnAvTmms, etc. It does not mean that they are still as common AMI NSM data objects. They are just parameter values which are composed of other objects and stored in a management server.

According to the above classification, an example how to construct 'detection logic' is shown in Fig. 1. The logic starts with 'EndDct' which indicate detection of an end device disconnected from AMI network, and eight results can be driven which are shown in Table IV. The correlation among objects is set forth in each diamond shape in Fig. 1 and the correlations of A and B which are too long to be described in the figure are the following:

-- A: [RsTmms – ConnTotTmms > threshold] ||
[ConnAvTmms < threshold] ||
[ConnFailTot < threshold]

-- B: [ConnExcAlm > threshold] || BufOvAlm

Table 4: Analysis Results of Anomaly From Fig. 1

# of Report	Causes	Related Objects
(1)	Network device or link error	[ConnAlm || ConnFailAlm] & RsTmms & ConnTotTmms & ConnAvTmms & ConnFailTot
(2)	Unknown failure of error	[ConnAlm || ConnFailAlm]
(3)	Resource exhaustion	[ConnAlm || ConnFailAlm] & RescExhAlm
(4)	Buffer overflow	[Conn || ConnFailAlm] & BufOvrfAlm
(5)	Resource exhaustion	[ConnExcAlm || ConnExcSimAlm] & [IdlTmmsMinAlm || IdlTmmsMaxAlm] & EndAlm
(6)	Unknown failure of error	EndAlm
(7)	End system error	EndAlm & EndLog
(8)	Buffer overflow	EndAlm & [BufOvAlm || BufUnAlm]

Fig. 1 and Table I made up of the original NSM objects from the IEC standard [2] appear short of precision, especially on the dotted line in Fig. 1. They can be reinforced with the objects newly defined in Table I, II and III, and the results are Fig. 2.

First, there is no decision if 'EndAlm' is not reported as shown in Fig. 1. However, we further analyze four more conditions: AddrResAlm, ConSigAlm, AuthProAlm, the condition 'D', and D is expressed as:

-- D: [UsrCurConnCnt] & [PduIdeCnt]

If 'AddrResAlm' is reported, C12.22 relay [28] does not seem to perform one of its duties - address resolution service. Otherwise, the next step, checking 'ConSigAlm', is executed, and we can decide whether any attack or abnormal control activity occur or not. If not, the authentication procedure needs to be inspected, and then 'CertInvAlm' or 'CrpOprAlm' will be checked in case of any failure during authentication procedure. No report of 'AddrResAlm', 'ConSigAlm', and 'AuthProAlm' makes the condition 'D' be checked. If D is met, resource exhaustion attack occurs by the only source which may be a root cause. If not, we can suspect program errors or unknown failure.

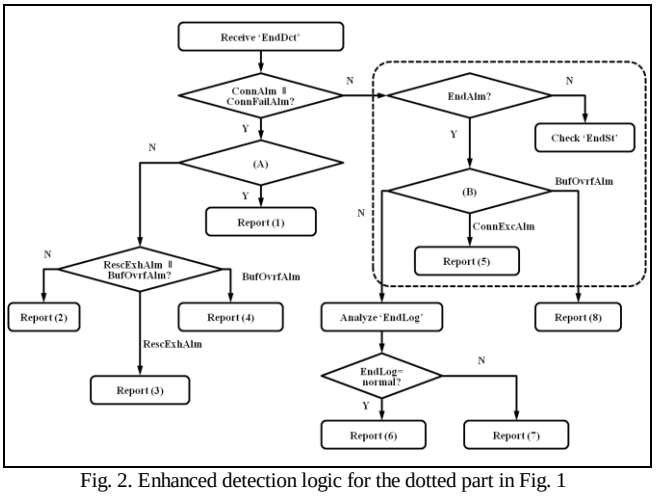

Fig. 2. Enhanced detection logic for the dotted part in Fig. 1

We define 17 more detection logics besides Fig. 1, and can enhance them with newly defined objects. The results are omitted here owing to the limited space.

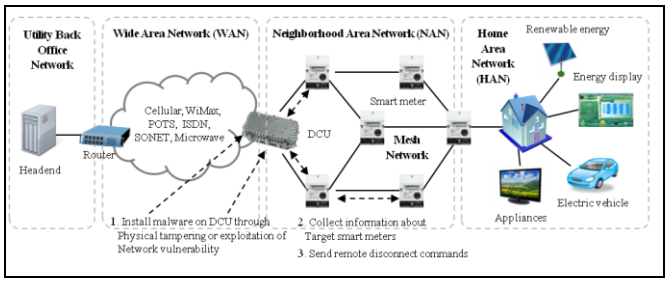

Fig. 3. Remote disconnect command attack scenario in [9]

4.2 Case Studies

It needs to check further whether or not the newly defined objects are useful on other attack scenarios. Here, two case studies are suggested with two scenarios.

Grochocki *et al*. [9] illustrated 'remote disconnect command attack through the Data Collection Unit' (Fig. 3), and we try to construct the corresponding detection logic as seen in Fig. 4.

In Fig. 3, malware is installed on Data Concentration Unit (DCU) through physical tampering or exploitation of network vulnerability, and then the malware collects information about target smart meters. Finally, the DCU is remotely controlled to send disconnect commands. The scenario is transformed to the detection logic in Fig. 4 for better understanding of the sequential attack story based on NSM objects.

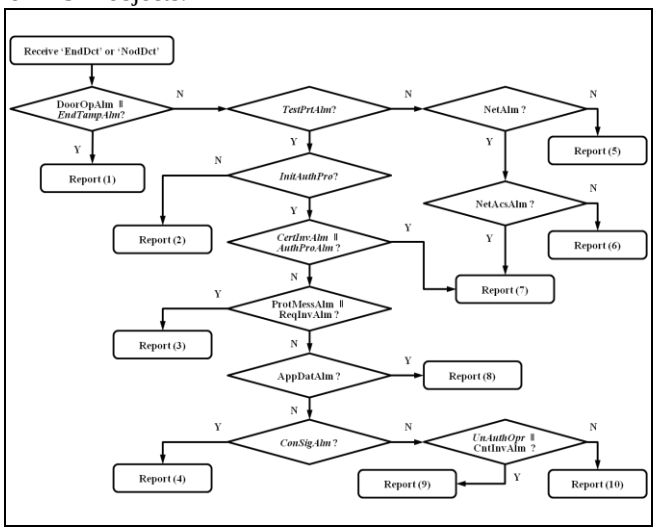

Fig. 4. Detection logic for the attack scenario in Fig. 3. Note that the italicized objects are newly defined in Table I, II and III

After receiving 'EndDct' or 'NodDct', physical tampering will be check through 'DoorOpAlm' or 'EndTampAlm'. For reference, physical tampering detection is required on every AMI device in Korea [33]. If none of two objects are reported, the intrusion through network interfaces can be suspected so that a configuration or test port should be checked with 'TestPrtAlm' object if the port is open and available. Otherwise, invalid network connection or access might occur.

Table 5: Analysis Results of Anomaly from Fig. 4

# of Report	Analysis results
(1)	Detection of physical tampering
(2)	Evasion attack by skipping authentication procedure
(3)	Unauthorized activity in excess of one's right
(4)	Illegitimate control command from HAN
(5)	Unknown failure or report error
(6)	New device connected without announcement in advance
(7)	Unauthorized device connected, but failed to access network
(8)	Software application error or complex attack detected
(9)	Unauthorized control in excess of one's right
(10)	Unknown failure, but not serious (keep monitoring)

If any test port is not available, the DCU is normally expected to initialize authentication procedure. Any failure during the procedure due to invalid certificates or other reasons will not allow further coming procedures to go on. That is all about the first step – malware installation in Fig. 3. In the second step where information about smart meters is collected, monitoring AMI application layer is desirable. 'ProtMessAlm', 'ReqInvAlm', and 'AppDatAlm' are within this scope. After there is information collected enough for meter attack, remote disconnect commands will be sent to the meter. It is advisable to confirm that any control signal from HAN should not be ruled out even though the protocol and data in application layer are sound. It makes sure that the disconnect commands are issued within NAN. Finally, the disconnect commands can be proved legitimate if neither 'UnAuthOpr' nor 'CntInvAlm' are reported. Table V gives additional information about Fig. 4.

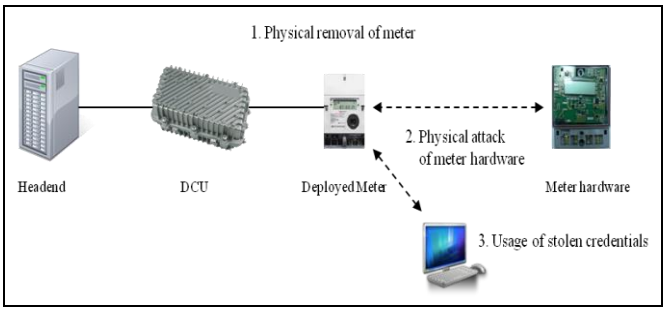

Fig. 5. Complex cyber-physical meter attack scenario in [3]

Two other scenarios can be founded in [3], and we choose one of them to describe detection logic: complex cyber-physical meter attack.

According to the proposed scenario in [3], attacker gains

physical access to a meter and removes it from the meter enclosure at first. Then, he/she attaches hardware and tools to the meter and obtain security information. By using the credentials, the attacker succeed in remote disconnect command after successful login. The detection logic for the attack can be constructed as seen in Fig. 5.

Table 6: Analysis Results of Anomaly from Fig. 5

# of Report	Analysis results
(1)	End system error, but not removal
(2)	End system is removed and lose power
(3)	Physical, but not logical connection to network
(4)	Evasion attack by skipping authentication procedure
(5)	Successful, but doubtful authentication
(6)	Temporal mistake in authentication procedure
(7)	Attack failed, and connection locked out
(8)	Attack in early stage, and more attempts expected
(9)	Attack in progress with security parameters like password
(10)	Unauthorized command or control, and attack in earnest

When attacker tries to remove a meter, 'EndTampAlm' is first reported, and 'EndDct', 'EndAlm', 'NetAlm' will follow. 'PwrLosAlm' is generated right after the meter is removed, of course. 'PwrOnAlm' and 'EndRs' indicate that the meter may be reinstalled there. During login trials, security processes are likely to fail several times. That makes security-related objects be reported. The objects are 'AuthProAlm', 'CertInvAlm', 'KeyInvAlm', and 'CrpOprAlm'. If the number of connection failure or login failure exceeds the predefined threshold, we have doubts about attack. After that, there is the potential for 'ChgAcsAlm' or 'ChgUsrAlm' to be reported. The final goal of the attack is to disconnect meters, and we can be aware of that activity through 'CntInvAlm' or 'UnAuthOpr'.

5. Conclusions

Electric devices become intelligent and work automatically rather than controlled manually in Smart grids. These facts have many advantages like demand control by AMI data or efficient power control through Flexible AC Transmission System (FACTS), but have also side effects like much higher possibility of cyber-attack because of its dependency on IT technologies. It can damage the availability and reliability of power system which is the most important in Smart grids, so it is inevitable to take measures against hostilities.

We propose common AMI NSM data object model and how to use it in monitoring AMI system. Newly defined objects and the detection logics based on them improve our awareness of what happens in AMI at the present. Two scenarios extracted from our references are used to give an instance of detection logic, and we verify that our detection logics with common AMI NSM data objects are of good use to analyze the current situation of AMI in details. It, of course, helps us to respond to cyber-attacks in time.

Anomaly detection method can make up for signature-based anomaly detection one in terms of unknown threats like zero day attacks. It is the key in anomaly detection how many scenarios we have so that the rate of successful detection rises through their detection logics. We have derived more than fifty attack stories from other references as well as [2], and developed prototypes that can support the common AMI NSM data object model. We plan to test our results in testbed, and then on the spot to verify and upgrade our research outcomes in the future.

References

[1] J.Liu, Y.Xiao, S.Li, W.Liang, C.L.P.Chen, "Cyber security and privacy issues in smart grid", IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp.981-997, 2012.
[2] IEC TC57, "Power system management and associated information exchange – Data and communications security – Network and System Management (NSM) data object models", IEC 62351 Part 7, 2010
[3] EPRI, "Advanced Metering Infrastructure common alarms
[4] and events", EPRI Technical Report, 2012.
[5] EPRI, "Intrusion detection system for Advanced Metering Infrastructures", EPRI Technical Report, 2012.
[6] EPRI, "Advanced Metering Infrastructure cyber security incident response guidelines", EPRI Technical Report, 2012.
[7] R.Alimi, Y.Wang, Y.R.Yang, "Shadow configuration as a network management primitive", in Proc. ACM SIGCOMM Conference on Data Communication, pp.111-122, 2008.
[8] M.A.Rahman, E.Al-Shaer, P.Bera, "A noninvasive threat analyzer for Advanced Metering Infrastructure in smart grid", IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 273-287, 2013.
[9] F.M.Cleveland, "IEC 62351-7: Communications and information management technologies – Network and System Management in power system operations", in Transmission & Distribution Conference and Exposition, 2008.
[10] D.Grochocki, J.H.Huh, R.Berthier, R.Bobba, W.H.Sanders, A.A.Cardenas, J.G.Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations", IEEE SmartGridComm Symposium, 2012.
[11] NIST, "NIST framework and roadmap for smart grid interoperability standards release 1.0", 2009.
[12] UCAlug: AMI-SEC Task Force, "AMI system security requirements v1.01", 2008.

[13] Congressional Research Service (CRS), "Smart meter data: privacy and cyber security", CRS Report for Congress, 2012.
[14] F.M.Cleveland, "Cyber security issues for Advanced Metering Infrastructure", in Proc. Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy, IEEE, 2008.
[15] S.McLaughlin, D.Podkuiko, P.McDaniel, "Energy theft in the Advanced Metering Infrastructure", Critical Information Infrastructures Security, Lecture Notes in Computer Science, vol. 6027, pp.176-187, 2010.
[16] M.Anas, N.Javaid, A.Mahmood, S.M.Raza, U.Qasim, Z.A.Khan, "Minimizing electricity theft using smart meters in AMI", IEEE International Conference on 3PGCIC, pp.176-182, 2012.
[17] S.S.S.R.Depuru, L.Wang, V.Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft", Energy Policy, vol. 39.2, pp.1007-1015, 2011.
[18] C.H.Kim, M.S.Choi, S.H.Ju, Y.H.Lim, J.M.Baek, "Security data extraction from IEC 61850 ACSI models for Network and System Management", Information Security Applications, Lecture Notes in Computer Science, pp. 142-150, 2012.
[19] UCAlug: AMI-SEC Task Force, "AMI system security requirements", 2008.
[20] UCAlug: AMI-SEC Task Force, "Security profile for Advanced Metering Infrastructure", 2010.
[21] Smart Grid Interoperability Panel (SGIP): Cyber Security Working Group, "Guidelines for smart grid cyber security", NISTIR 7628, 2010.
[22] UCAlug: SG Net SRS, "Smart grid networks system requirements specification", 2010.
[23] Department of Homeland Security, "Catalog of control systems security: recommendations for standards developers", 2010.
[24] R.Berthier, W.H.Sanders, H.Khurana, "Intrusion detection for Advanced Metering Infrastructures: requirements and architectural directions", IEEE International Conference on Smart Grid Communications, 2010.
[25] R.Berthier, W.H.Sanders, "Specification-based intrusion detection for Advanced Metering Infrastructures", 17th Pacific Rim International Symposium on Dependable Computing, IEEE, 2011.
[26] P.McDaniel, S.McLaughlin, "Structured security testing in the smart grid", 5th International Symposium on Communications, Control and Signal Processing, 2012.
[27] F.M.Tabrizi, K.Pattabiraman, "A model for security analysis of smart meters", IEEE International Conference on Dependable Systems and Networks Workshops, 2012.
[28] S.Rana, H.Zhu, C.W.Lee, D.M.Nicol, I.C.Shin, "The not-so-smart grid: preliminary work on identifying vulnerabilities in ANSI C12.22", IEEE Globecom Workshops, 2012.
[29] American National Standard Protocol Specification for Interfacing to Data Communication Networks, ANSI C12.22-2008, 2008.
[30] American National Standard Protocol Specification for ANSI Type 2 Optical Port, ANSI C12.18-2006, 2006.
[31] American National Standard for Utility Industry End Device Data Tables, ANSI C12.19-2008, 2008.
[32] Korea Electric Power Corporation, "KEPCO AMI specifications for data concentrator unit & PLC modem", 2012.
[33] B.Schneier, "Attack Trees: Modeling security threats", Dr. Dobb's Journal, 1999.

Seongho Ju received the B.S. degree in electrical engineering from Yonsei University, Seoul, Korea, in 2001, and the M.S. degree in electrical and computer engineering from Seoul National University, Seoul, in 2004. Since he joined Korea Electric Power Cooperation in 2004, he has developed power-line communication, network management system, and especially AMI system as a Senior Researcher. He is a member of WG 15 in TC57, and his recent research areas are in the security system for SCADA, SA, DAS as well as AMI.

Yonghun Lim received the B.S. and M.S. degrees in electronic engineering from Konkuk University, Seoul, Korea, in 1996 and 1998, respectively. He joined Korea Electric Power Corporation in 1996. He has worked on optic network, wireless sensor network, and radio frequency identification/ubiquitous sensor network as a project leader. His recent research topic is anomaly detection and response in Substation Automation System.

Chunghyo Kim received the B.S. degree in electronic engineering from Korea University, Seoul, Korea, in 2003, and the M.S. degree in electronic engineering from Korea Advanced Institute of Science and Technology, Daejeon, in 2005. In 2005, he joined Korea Electric Power Corporation, and he developed Network and System Management (NSM) data object model to monitor and manage power system. His current research focuses on security system for Substation Automation System.

Kyungseok Jeon received the B.S. degree in electronic engineering from Hanyang University, Seoul, Korea, in 1986, and the M.S. degree in Information & communication engineering from Korea University, Seoul, in 2001. Since 2013, he has been a principal researcher with Korea Electric Power Corporation, Korea. His research interests include security & network system for SA and AMI.