ANALYZING THE EFFECTS OF VARIOUS ATTACKS ON SMART METERS

Mohsen ZABIHI
MEEDC - Iran
m.zabihi@meedc.net

Mahsa TAVASOLI
MEEDC - Iran
m.tavasoli@stu.um.ac.ir

Mohammad Hossein YAGHMAEE
MEDDC - Iran
h.yaghmaee@um.ac.ir

Marziyeh TAVASOLI
MEEDC - Iran
marziyetavasoli@ut.ac.ir

ABSTRACT

Meters contain important data which flow in network structure. Therefore, there are always attacks that challenge availability, integrity and confidentiality which are the most important security requirements of meters. Scales of effects of various attacks on contravention of the requirements are different.

The main purpose of the current study is to evaluate the total effects of various attacks on meters. In order to distinct the most dangerous attack, logical decision making methods have to be utilized in this paper. Because of complexity of the issue and existence of different alternatives and quantitative and qualitative criteria, the method of analytical hierarchy process (AHP) has been selected.

1-INTRODUCTION

Smart meter is an advanced energy meter that measures the energy consumption of a consumer and provides added information to the utility company compared to a regular energy meter. Smart meters can read real-time energy consumption information including the values of voltage, phase angle and the frequency and securely communicates that data. The ability of smart meters for bidirectional communication of data enables the ability to collect information regarding the electricity fed back to the Power grid from customer premises.

They can also collect diagnostic information about the distribution grid, home Appliances, and can communicate with other meters in their reach. They can measure electricity consumption from the grid, support decentralized generation sources and energy storage devices, and bill the customer accordingly. Data collected by smart meters is a combination of parameters such as a unique meter identifier, timestamp of the data, and electricity consumption values. Smart meters can be programmed such that, only power consumed from the utility grid is billed while the power consumed from the distributed generation sources or storage devices owned by the customers is not billed. Smart meters can limit the maximum electricity consumption and can terminate or re-connect electricity supply to any customer remotely [1,2]. Fig.1 shows an architectural model of a conventional energy meter and a smart meter [3]. The cyber security working group in the NIST Smart Grid interoperability panel has recently released a comprehensive guideline for smart grid cyber security [4]. In the following, we cite three high-level smart grid security objectives.

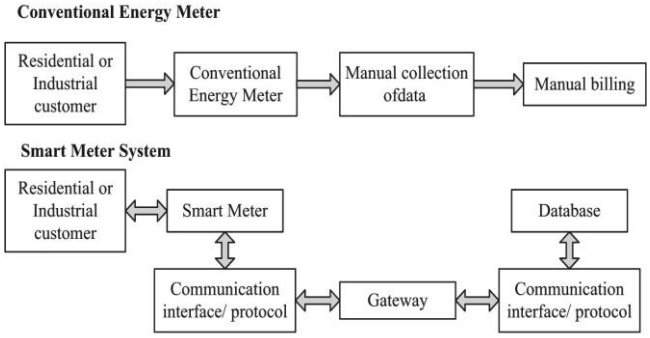

Fig.1 an architectural model of a conventional energy meter and a smart meter.

Availability: Ensuring timely and reliable access to the meter and use of information are the most importance issues in the smart grid. This is because a loss of availability is the disruption of access to or use of information, which may further undermine the power delivery.

Integrity: Guarding against improper information modification or destruction is to ensure information nonrepudiation and authenticity. A loss of integrity is unauthorized modification or destruction of information and can further induce incorrect decision regarding power management.

Confidentiality: Preserving authorized restrictions information access and disclosure is mainly to protect personal privacy and proprietary information. This is in particular necessary to prevent unauthorized disclosure of information that is not open to the public and individuals.

Meters contain important data which flow in network structure. Therefore, there are always attacks that challenge confidentiality, integrity and availability which are the most important security requirements of smart grid.

The Advanced Metering Infrastructure (AMI) is used to connect customers' homes, the utility center and the electricity market. In the AMI network, message delivery becomes non-time critical and availability is less important than integrity and confidentiality. Thus, network security approach for the AMI network should focus primarily on integrity and confidentiality. Scales of

effects of various attacks on contravention of the requirements are different. The remaining of this paper is organized as follows:
In section 2 we introduce some important attacks on smart meters. In section 3 we present the method for analyzing the effects of various attacks on smart meters. Finally, we discuss and conclude in section 4, respectively.

2-ATTACKS ON SMART METER

In the context of smart metering, security objectives are different from others smart grid operations. Data sent by smart meters is sensitive and need to be protected from attackers.
Therefore, a number of smart meters can be configured to operate in different security modes [5]. The remainder of this section introduce some important attacks on smart meters.

2-1-Remote connect/disconnect (RCD)

Smart meters are one of the most visible elements of the transition to a modern smart grid. Across the United States and Europe, and increasingly in other parts of the world as well, millions of smart meters have been deployed as utilities invest in Advanced Metering Infrastructure (AMI) to enable dynamic pricing, remote service switching, and other services. Smart meters are typically controlled and queried through wireless or power-line communication. However, this communication and remote control capability also introduces potential attacks with severe consequences for consumers and asset owners. In particular, the service switch and associated remote connect/disconnect (RCD1) capability of smart meters has caught the attention of the security community in recent years [6-9]. An RCD attack could cause a widespread blackout (or blackmailing of such a blackout) [6], or could potentially harm the power network or other loads by causing voltage or frequency deviations [7]. In either case, a successful attack would have severe economic and political consequences. While security measures like data encryption and Intrusion Detection Systems (IDS) offer some level of protection for AMI systems, they provide little recourse if an attacker is able to compromise the system and issue malicious disconnect.

2-2-Framework upgrade

To manage change in a dynamically growing smart grid, it is essential to be able to remotely upgrade firmware, such as that found in meters, without replacing the equipment or manually performing this in the field. Remote image download capability will permit certain characteristics of the meter to be substantially altered on an as-needed basis [10]. The other side of firmware upgrades is that they serve as a powerful tool for attackers, if they can be abused. For example, an attacker who can push his own firmware to other meters can execute a disconnect action and then make the meter completely unresponsive till it is returned to the manufacturer, thus making it impossible for the network operator to reverse his actions [11].

2-3-Replay attack in smart meter

Since the communication medium within the HAN is wireless communication, this introduces a number of unique security vulnerabilities for the communication between smart meter and home devices.
Replay attacks can be more damaging and successful than mere eavesdropping because they can cause remote actions even against cryptography. The basic idea of a replay attack is to capture packets sent on a wireless or wired between two hosts with the intent to later to replay the payloads (or more rarely the same packets) in order to affect the same result [12]. Replay attacks can change authentication packets and pretend the legal identification
It causes spoofing security certification and making illegal access to the control system [3].

2-4-Meter Spoofing

One risk of placing a physically insecure device on a network is the potential for a spoofing attack, in which another adversarial device impersonates the legitimate one. The studied system uses the standard ANSI C12.21 protocol for mutual authentication of meters and utilities. In this protocol, the meter creates a cryptographic nonce which is sent to the utility. The energy utility software then computes a Message Authentication Code (MAC) by hashing the password and nonce. The calculation is done using the ANSI X3.92-1981 data encryption algorithm [13]. The MAC is then sent to the meter which calculates its own MAC which is sent to the utility software. At this point, mutual authentication is complete. The flaw in the studied system in [14] is that the utility software does not verify the freshness of the nonce from the meter. Thus, an adversary that is able to eavesdrop on an authentication session can replay the nonce and authenticate itself as the meter. In Fig.2, a reply attack example is shown.

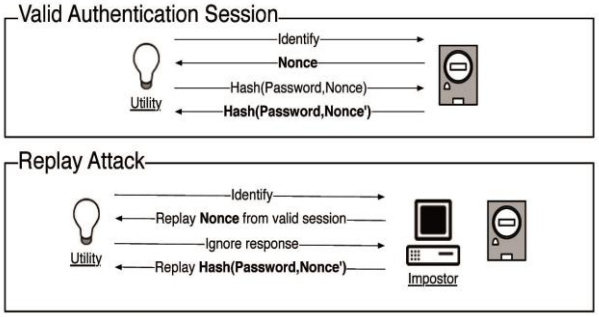

Fig.2.Replay attack example

2-5-Eavesdropping, Communication interception and trafic analysis

It is interposition the attacker on the backhaul network. Interposition is needed for any passive attack, including capturing the protocol between meters and utilities for reverse engineering. Network interposition can most easily be achieved close to one of the endpoints. For customers, tapping a line between the meter and the first backhaul link is the easiest. Utility insiders would have ready access to the links and routers leading up to the computers performing remote meter reads [14].

3-METHOD

The main purpose of the current study is to evaluate the total effects of various attacks on meters. In order to distinct the worst attack, logical decision making methods have to be utilized in this paper. As for complexity of the issue and existence of different alternatives and quantitative and qualitative criteria, the Analytical Hierarchy Process (AHP) method has been selected.

3-1- The Analytical Hierarchy Process (AHP)

The Multi-Criteria Decision Making (MCDM) methods deal with the process of making decision in the presence of multiple criteria or objective. Analytical hierarchy process (AHP), is one of the most well-known multi-criteria decision making techniques [15]. Most of the MCDM techniques require numerous parameters, which are difficult to be determined precisely requiring extensive sensitivity. How to deriving priority vector from a pairwise comparison matrix has being an important research topic in the AHP and is substantially investigated in the AHP literature Whenever the act of decision making faces various competent alternatives and criteria for making decisions, this method may be applied. Considered criteria can be either quantitative or qualitative. This technique is based on pairwise comparison [15].

Moreover, inherent in the AHP is the ability to handle input from multiple decision makers. Furthermore, the security properties may be competitive benchmarking for AHP. For example, the security holes and the cryptography strength are competitive benchmarking, the security degree of target system are reduced with the in-creasing of security holes, but enhanced with the increasing of cryptography strength [16].

We analyzed the effects of various attacks on smart meters and then select one of them as dangerous attack. This conclusion can enable companies to optimize protection ways for different meters.

At first we should analyze the effects of various attacks on availability, confidentially and integrity of smart meters. Briefly, the step-by-step procedure in using AHP is as follows:

Step 0:

In the current study, goal is selection of the most dangerous attacks and criteria are CON=***confidentiality,*** INT= ***integrity***, and AVA=***availability*** and here, alternatives are the attacks which are performed on meters 1= **RCD**, 2= **framework upgrade**, 3=**replay attack**, 4=**smart spoofing**, 5= **Communication interception and traffic analysis**. At this step we define decision criteria in the form of a hierarchy of objectives. The hierarchy is structured on different levels:

From the top (i.e. the goal) through intermediate levels (criteria and sub-criteria on which subsequent levels depend) to the lowest level (i.e. the alternatives). Fig.3 show hierarchy structure adopted for most dangerous attack of smart meter.

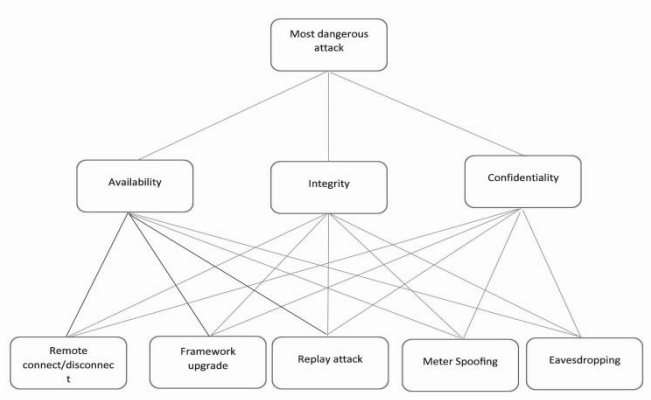

Fig.3 hierarchy structure for most dangerous attack of smart meter

Step 1:

Weight the criteria and alternatives as a function of their importance for the corresponding element of the higher level. In this step we weighted the alternatives and the criteria by assessments of experts by questionnaire [17, 18].

Step 2:

In pairwise comparison, the attacks at level three have to be compared for each criteria in a pairwise manner. Pairwise comparison is performed in a design for identical Distinction up to limitless distinct. As a sample, Table.1 shows part of judgment matrix for alternatives with respect to confidentiality and confidentiality judgment matrix.

The proposed solution for pairwise comparisons is to design queries which are based on determination of importance degree of pairwise alternatives and criteria. After collection of the queries, geometric mean, the following formula is applied to combine the results and change them to a group judgment matrix. Geometric mean is the most proper mathematical rule for combining

the judgments in AHP.

$$a_{ij} = \pi_{K=1}^{N} a_{ij} (K^{\frac{1}{N}}) \quad (1)$$

Table 1: (A). sample of judgment matrix for alternatives with respect to confidentiality by an expert,
(B). sample of confidentiality judgment matrix

	PI				
CON	1	2	3	4	5
1	1	1	1	1	0/4
2	1	1	1	1	0/4
3	1	1	1	1	0/4
4	1	1	1	1	0/4
5	2/5	2/5	2/5	2/5	1

(A)

CON	1	2	3	4	5
1	1/00	1/32	1/26	1/74	1/45
2	0/76	1/00	0/83	1/32	1/10
3	0/79	1/20	1/00	1/38	1/15
4	0/57	0/76	0/72	1/00	0/83
5	0/69	0/91	0/87	1/20	1/00

(B)

Step 3:
After a judgment matrix has been developed, a priority vector to weight the elements of the matrix is calculated. This is the normalized eigenvector of the matrix. See Table2.

Table 2: (A) the normalized eigenvector of group matrix
(B) the normalize eigenvector of criteria judgment matrix

CON	1	2	3	4	5	TOTAL		eigenvector
1	1/00	1/32	1/26	1/74	1/45	7/77	1/332602	0/26205
2	0/76	1/00	0/83	1/32	1/10	7/01	0/982307	0/193166
3	0/79	1/20	1/00	1/38	1/15	8/52	1/085704	0/213499
4	0/57	0/76	0/72	1/00	0/83	7/89	0/765379	0/150508
5	0/69	0/91	0/87	1/20	1/00	9/67	0/919315	0/180779

(A)

	CON	AVA	INT	TOTAL	priority	eigenvector
CON	1/00	7/00	0/33	8/33	1/318232314	0/304718182
AVA	0/14	1/00	0/14	1/29	0/276771022	0/063977466
INT	3/00	7/00	1/00	11/00	2/73106708	0/631304352

(B)

Step 4:
Inconsistency ratio, the AHP enables the analyst to evaluate the goodness of judgments with the inconsistency ratio IR. The judgments can be considered acceptable if IR $<= 0.1$. In this case IR for group matrix in respect of criteria is 0.03, 0.002 and 0.00000001.see Table3.

Step 5 finding the most dangerous attack:
And finally, once the comparisons and weighting of alternatives are accomplished, the most weighted alternative will be defined as the most dangerous alternative. As shown in Table.4, communication interception and traffic analyze is dangerous one. This is because their weighted average is higher.

Table 3: a sample, IR for judgment group matrix in respect of confidentially

CON	1	2	3	4	5	priority	WSV	CV
1	1/00	1/32	1/26	1/74	1/45	0/26	1/31	5/00
2	0/76	1/00	0/83	1/32	1/10	0/19	0/97	5/00
3	0/79	1/20	1/00	1/38	1/15	0/21	0/86	4/03
4	0/57	0/76	0/72	1/00	0/83	0/15	0/75	5/00
5	0/69	0/91	0/87	1/20	1/00	0/18	0/90	5/00
							λ_{MAX}	4/81
							CI	0/04
							IR	0/03

Table 4: AHP final ranking for four attacks

Criteria / Attack	CON	AVA	INT	Weighted average for each attack
	0/304718	0/063977	0/631304352	
1- Smart meter RCD	0/26205	0/173717	0/182256527	0/206024656
2-Framework upgrade	0/193166	0/218365	0/172066111	0/181457679
3-Replay attack	0/213499	0/167208	0/174182883	0/185716861
4-Meter spoofing	0/150508	0/216352	0/201715689	0/18704822
5-Communication interception and traffic analysis	0/180779	0/22437	0/28868365	0/251688468

4-CONCLUSION

Meters contain important data which flow in network structure. Therefore, there are always attacks that challenge availability, integrity and confidentiality. In the context of smart metering, security objectives are different from others smart grid operations. . In the AMI network, message delivery becomes non-time critical and availability is less important than integrity and confidentiality. Data sent by smart meters is sensitive and need to be protected from attackers. Some of these attacks used in analyzing are RCD, framework upgrade, replay attack, smart spoofing, communication interception and traffic analysis.
The main purpose of the current paper was to evaluate the total effects of above attacks respect to availability, integrity and confidentiality on meters. For distinction the most dangerous attack, logical decision making methods have to be utilized in this paper. The result of AHP method confirm that «Communication interception and trafic analyses» are dangerous attacks.

REFERENCES

[1] A.Vojdani, "Smart integration", IEEE Power & Energy Magazine November 2008.
[2] D.G.Hart, 2008," Using AMI to realize the smart grid". In: Proc. IEEE Power and Energy Society General meeting Conversion and Delivery of Electrical Energy,p.

1–2.
[3] L.Z. Sh.Chen, 2012," A Survey of Research on Smart Grid Security", Communications in Computer and Information Science, pp. 395–405.
[4] "The Smart Grid Interoperability Panel–Cyber Security Working Group, Guidelines for smart grid cyber security", NISTIR7628 (2010)1–597.
[5] Z.Ismail, J.Leneutre, D.Bateman, L.Chen, 2014," A Game Theoretical Analysis of Data Confidentiality Attacks on Smart-Grid AMI", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 32, NO. 7, JULY.
[6] R. Anderson, S. Fuloria, 2010, "Who controls the off switch?" *SmartGridComm Conference.*
[7] M. Costache, V. Tudor, M. Almgren, M. Papatriantafilou, C. Saun- ders, 2011, "Remote control of smart meters: friend or foe?" *in Proc. of the European Conference on Computer Network Defense (EC2ND).*
[8] D. Grochocki, J. H. Huh, R. Bobba, W. H. Sanders, A. A. Cardenas, and J. G. Jetcheva, 2012, "AMI threats, intrusion detection requirements and deployment recommendations" *SmartGridComm Conference.*
[9] W.G.Temple, B.Chen, N.O.Tippenhauer, 2013, "Delay Makes a Difference: Smart Grid Resilience under Remote Meter Disconnect Attack", *IEEE SmartGridComm Symposium.*
[10] A.F.Snyder, B.Rankin, I.B.Snyder, T.Swain, 2014, "The realities of testing meter firmware upgradeability", *Power Systems Conference (PSC).*
[11] "The Dark Side of the Smart Grid Smart Meters (in) Security", www.c4-security.com.
[12] G.A.Tizazu, H.R.Hussen, K.H.Kim, 2013," Secure Session Key Exchange Scheme for Smart Grid Home Area Networks", *ICT Convergence (ICTC), International Conference on*, Page(s): 1116 – 1120.
[13] American National Standards Institute: ANSIX3.92-198 Data Encryption Algorithm (1981).
[14] S.McLaughlin, D.Podkuiko, and P.McDaniel, "Energy Theft in the Advanced Metering Infrastructure ", Springer-Verlag Berlin Heidelberg 2010, pp. 176–187, 2010.
[15] R.Ramanathan, 2006," Data envelopment analysis for weight derivation and aggregation in the analytic hierarchy process",Comput Oper Res 33:1289–1307.
[16] N.Liu, J.Zhang, H.Zhang, W.Liu, 2010, "Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM", IEEE Transactions on Power Delivery,pp: 1492-1500.
[17] W.Wang, Z.Lu, 2013," Cyber security in the Smart Grid: Survey and challenges ", Computer Networks 57, p: 1344–1371.
[18] S.S.Depuru, L.Wang, V.Devabhaktuni, 2012, "Smart meters for power grid: Challenges, issues, advantages and status", Renewable and Sustainable Energy Reviews 15, pp: 2736–2742