Risk Analysis Model for Smart Meters in Electrical Power Distribution Systems

Mirza Šarić [1]

[1]*JP EP BiH - d.d. Sarajevo, Adema Buća 34, Mostar Bosnia and Herzegovina*

Abstract **– Smart meter installation is one of the largest engineering projects in the world. It is expected to provide numerous possibilities for the power system modernization, management and operational advancement. However, installation of smart meters introduces an unprecedented level of exposure to risk. This paper proposes the application of Mamdani type fuzzy inference in modelling the risk for smart meter attack. The proposed model takes into consideration customer sensitivity and consumption patterns. It is argued that this paper provides a model which can contribute towards more comprehensive smart meter risk analysis and mitigation strategies. This paper demonstrates that the intrusion detection for smart meters is an important and vibrant research area with numerous research opportunities.**

Keywords **– Distribution system, Fuzzy system, Intrusion detection, Risk, Smart meter**

1. Introduction

Modern power systems are going through the period of biggest organizational, structural and technological changes in their history. These changes are driven by the processes of market liberalization and energy transition. The introduction of smart meters is considered to be the largest engineering project in EU, with an expected cost of more than $100bn for its 27 Member States [1]. This project is expected to provide numerous advantages such as remote meter access, demand response and real time pricing. On the other side of the ocean, US administration is securing billions of dollars towards the modernization of power systems [2]. Utilities find smart meter data beneficial for numerous operational activities such as outage management, planning and billing. However, there is a long way to go because there are numerous challenges that still need to be appropriately addressed. Lack of communication between meters and appliances, for example, could significantly limit the benefits of demand response [1].

Power system technical modernization in terms of information and communication technologies advancement promises to provide significant benefits to both, customers and system operators. However, installation of smart meters and Advanced Metering Infrastructure (AMI) in general, introduces an unprecedented level of exposure to risk of the power system components, which have the potential to cause considerable damage and interruption of power supply. AMI introduction extends the set of existing vulnerabilities, some of which were not accounted for in the early stages of the system development, to new cyber threats since it is no longer required to have physical access to equipment. From a utility's perspective, it is becoming increasingly important to perform relevant risk analysis of the system and propose appropriate mitigation strategies. This paper investigates some of the most common smart meter threats and proposes the application of Mamdani type fuzzy inference in modelling the risk of smart meter attack.

2. Overview of AMI and IDS

The main role of an AMI is to enable communication between the utility control centre and the smart meters. The main components of AMI are smart meters, data concentrators, communication media/networks, central system and all these components are located in both public and private realms [3]. Smart meters are designed to record, send and receive a wide range of information, such as remote reading, price information alerts, outages information and upgrades [4]. In order to facilitate

DOI: 10.18421/SAR11-03
https://dx.doi.org/10.18421/SAR11-03

Corresponding author: Mirza Šarić,
JP EP BiH - d.d. Sarajevo, Adema Buća 34, Mostar Bosnia and Herzegovina
Email: midjisaric@gmail.com

Received: 17 January 2018.
Accepted: 11 February 2018.
Published: 21 March 2018.

communication, meter architectures are designed for a wide range of communication media. It is a hierarchical system which consists of numerous interconnected networks such as the Home Area Network (HAN), Neighborhood Area Network (NAN) and Wide Area Network (WAN).

Intrusion detection system (IDS) can be defined as a system used to detect any activity which might jeopardize the security of the observed system. The most important task of an IDS is to detect the intrusion before serious damage is done to the systems. In terms of high level structure, IDS consists of three functional components: an information source, an analysis engine and a decision maker [5] and can be implemented as hardware or software solutions. Therefore, IDS can be classified with regards to intrusion detection techniques, architecture and the response [6]. Further, IDS can be classified into two categories based on the model of intrusion and the data source [7]. Fig. 1 shows a high level IDS classification diagram based on [7].

IDS based on artificial intelligence tools, such as fuzzy logic, artificial neural network, generic algorithms, are emerging at rapid paste. Application of fuzzy systems has some important advantages because it can use large amounts of data as input space and map it to the output space with high tolerance to imprecision and soft approach to boundary conditions. Fuzzy intrusion detection systems can be used to identify port scanning, denial of service attacks and detect some types of backdoor and Trojan horse attacks [5]. They are essentially anomaly based systems. Even if the anomaly based assessment is complex, it was shown that fuzzy systems can be used to detect several classes of intrusive behaviour using the anomaly-based approach [5]. It was shown that the dynamic approach is capable to discover known or unknown intrusion patterns [8]. Conventional ID methods, based on current intrusion detection techniques, mainly focus on discovering abnormal system events [8].

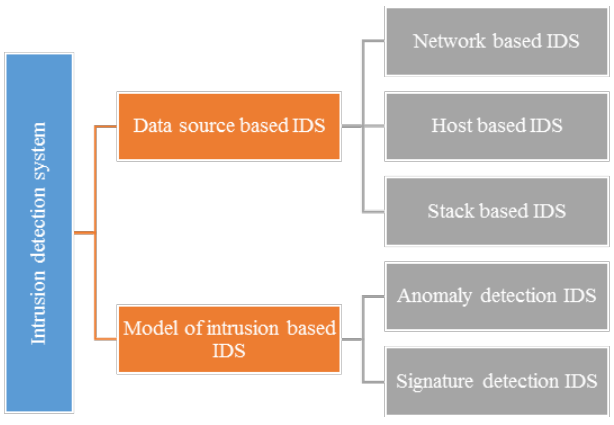

Figure 1. Intrusion detection system classification

The fuzzy logic approach is useful in constructing management models and trade-off between attack detection rate and cost of inter-device communication [9]. Application of fuzzy IDS as a high level system monitoring, in combination with other smaller systems, appears to be a promising area of research and applications [5]. The major motivation for the introduction of IDS based on artificial intelligence tools lies in the fact that none of the existing methods are completely flawless and the search for improvements continue.

3. Threat definition and evaluation

Risk in general terms can be defined as an exposure to danger, or as the possibility that something unpleasant or unwelcome will happen while the risk management can be defined as forecasting and evaluation of financial risks together with the identification of procedures to avoid or minimize their impact [10]. Therefore, defining P as the probability and C_q as the consequence of an unwelcome event, a risk can be expressed:

$$R = P \times C_q \tag{1}$$

Smart meters handle potentially sensitive incoming and outgoing information such as real time power usage, which is privacy sensitive and off switch operation which is security sensitive. Utilities express the controllability over AMI devices to be their primary security concern, right before the loss of observability caused by a lack of data integrity [11]. They are further concerned regarding the over regulation which increases the costs while providing little benefit [1]. One of the most important threats to the AMI system is electricity theft with an estimated cost of over $25 billion every year [12]. The introduction of an AMI makes the power system more vulnerable to electricity theft because it offers new ways and approaches for performing the actual theft [13]. The possible attacker could include electricity customers, who have an incentive to lower their usage, organized crime, unsatisfied utility employers and even terrorists. Attackers can also be intrusive data management and marketing agencies, swanky attackers, malicious and curious eavesdroppers [12].

4. Fuzzy model proposition

Within the boundary of classical set theory, membership of an object to a set is precisely defined quantity. In a fuzzy domain, there is a much softer approach to membership concept which recognizes values of graded membership. Considering the classical set *A* of the universe U, and if we define

$\mu_A(x)$ as a function called membership function which specifies the grade or degree to which any element x in *A* belongs to the fuzzy set A, then we can define a fuzzy set A or ordered pairs, a binary relation as [14]:

$$A = \{(x,\mu_A(x))|x \in A, \mu_A(x) \in [0,1]\} \quad (2)$$

Fuzzy systems can be employed in numerous engineering applications such as control, supervision planning and multi criteria decision making. In this paper, a fuzzy model, shown in Figure 2, is proposed as a tool for risk assessment. In the proposed model, the input and output linguistic variables are described by an expert knowledge and represented by sets A, B and C which contain single terms A_i, B_j i C_k [14]:

$$\begin{aligned} A &= \{A_1, A_2, \cdots, A_i, A_{i+1}, \cdots, A_n\} \\ B &= \{B_1, B_2, \cdots, B_j, B_{j+1}, \cdots, B_m\} \\ C &= \{C_1, C_2, \cdots, C_k, C_{k+1}, \cdots, C_l\} \end{aligned} \quad (3)$$

Terms A_i, B_j i C_k are fuzzy sets defined as [14]:

$$\begin{aligned} A_i &= \{(x, \mu_{Ai}(x))|x \in A_i \subset U_1\}, \quad i = 1, \cdots, n \\ B_j &= \{(y, \mu_{Bj}(y))|y \in B_j \subset U_2\}, \quad j = 1, \cdots, m \\ C_k &= \{(z, \mu_{Ck}(z))|z \in C_k \subset U_3\}, \quad k = 1, \cdots, l \end{aligned} \quad (4)$$

In electrical power distribution systems, customers have different response to outages depending on how much they rely on electricity during the period of interruptions and how serious the damage caused by service interruption might be. In some cases, service interruption in electricity distribution systems can result in serious injuries, deaths, prosecutions and permanent losses with large public, environmental and financial consequences which means that it is important to recognize significance of customer sensitivity [10] in system management. In this paper, a customer sensitivity matrix developed and presented in [10] is used to represent different levels of customer sensitivity. When planning the appropriate risk mitigation strategy, it is important to take into consideration customer sensitivity as one of the most important criteria. With reference to the equations (3) and (4), customer sensitivity is represented in this paper with following fuzzy sets [10]:

$$CS = \{A_1, A_2, A_3, A_4, A_5\} \quad (5)$$

$$CS = \{\text{verylow, low, average, high, veryhigh}\} \quad (6)$$

The second input variable in the proposed Mamdani type model is the monthly energy consumption. This variable is introduced in the model because it is proposed that customers with larger energy usage pose a greater risk in the case of an unwelcome event. Maximum energy consumption data are retrieved from the utility data base and normalized into (0-1) range where the highest value is associated with a value of 1, which corresponds to the maximum value of 10000 kWh. The smallest value is associated with a value of 0 and it corresponds to consumption of 0 kWh. The limits of the set are chosen arbitrarily and it is assumed that most domestic and small business customers will fall within this range. The values are normalized in order to provide model flexibility. In this way, it would be trivial to extend the values to any desired range without affecting the underlying logic. The proposed model is therefore flexible and can be used to include any desired value. The second input variable is represented by a set E as follows:

$$E = \{B_1, B_2, B_3, B_4, B_5\} \quad (7)$$

$$E = \{\text{verylow, low, average, high, veryhigh}\} \quad (8)$$

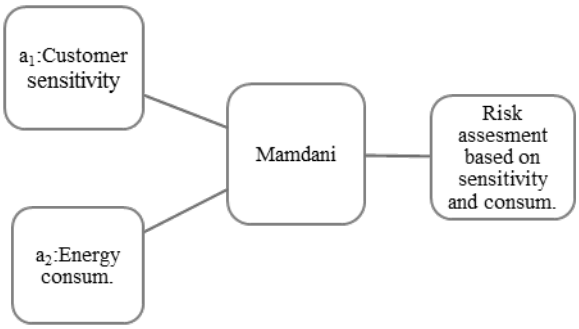

Figure 2.Mamdani type fuzzy inference for risk assessment

Output variable represents the quantitative measure of risk assessed based on the customer sensitivity and energy consumption. The output variable of the proposed system can be used as criteria for ranking the IDS solution project and for risk mitigation strategy planning. Defuzzification stage provides final control output value of the fuzzy model procedure. Output variable is represented by set RISK, shown below. Graphical representation of the input and output variables is shown in Figure 3.

$$RISK = \{C_1, C_2, C_3, C_4, C_5\} \quad (9)$$

$$RISK = \{\text{verylow, low, average, high, veryhigh}\} \quad (10)$$

Table I shows IF…AND…THEN rules which are used to obtain output variable described by the set C. In this case, n and m are the numbers of elements of input variable sets, and give a total of 5*5=25 rules.

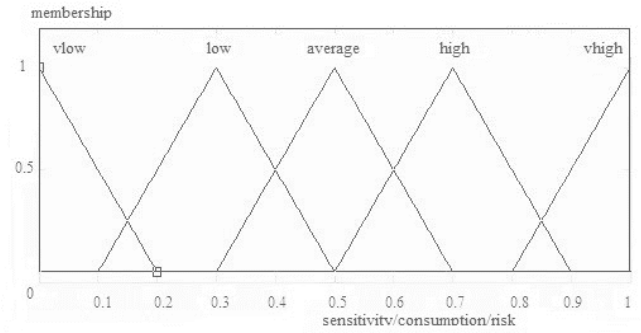

Figure 3. Representation of input and output variables

Table 1: Fuzzy rules

Energy Consumption	Customer Sensitivity VLow	Low	Average	High	VH
V Low	**VL**	**VL**	**L**	**L**	**H**
Low	**VL**	**L**	**A**	**H**	**VH**
Average	**L**	**A**	**H**	**H**	**VH**
High	**L**	**A**	**H**	**H**	**VH**
VH	**A**	**A**	**H**	**VH**	**VH**

5. Model application and discussion

Final simulation results can be summarized in surface view shown in Fig. 4. For a given value of customer sensitivity and energy use, Fig. 4 shows the required output value, which represents the risk level. This output value is used as a control output to rank the meters in the desired network section according to the prescribed criteria.

The accumulated body of evidence suggests that fuzzy tools play an important role in IDS because they can take advantage of our tolerance to imprecision and uncertainty [8]. The further literature survey indicates that fuzzy models are capable to deduce behavioral patterns and form a relationship between input and output space which is obvious, but cannot be easily described with classical mathematical tools. This statement is particularly applicable to the electrical power distribution network planning problem which is a preference based decision making process and involves an assessment of complex criteria [15]. One of the important modern planning criteria is the risk evaluation. For the reasons discussed in this paper, the modern planning requirements extend the need for risk analysis beyond the standard line replacement and reconstruction projects, to the smart meter management projects. It is required from decision makers to make decisions of both strategic and operational importance, such as the meter replacement priority, intrusion prevention and detection technology deployment such as the grid-placed sensors described in [16]. This paper proposed a model which can be applied to realistic data obtained from the Electrical Distribution Company. The information obtained from this model can be used as valuable decision support inputs in the process of smart meter management. In order to show its practical application, let us consider that we have a particular customer whose consumption is 2,000 kWh per month and whose sensitivity is assessed to be 0,45. The application of the proposed model gives an output of 0,431 which is used to rank customer for planning purposes, based on this particular criteria. Graphical representation is space demanding and it is omitted in this paper. The advantage of the method is that it can be used to automatically process large amount of data which is important for distribution system applications. This model is flexible and can be extended to include other data range and criteria required by decision makers.

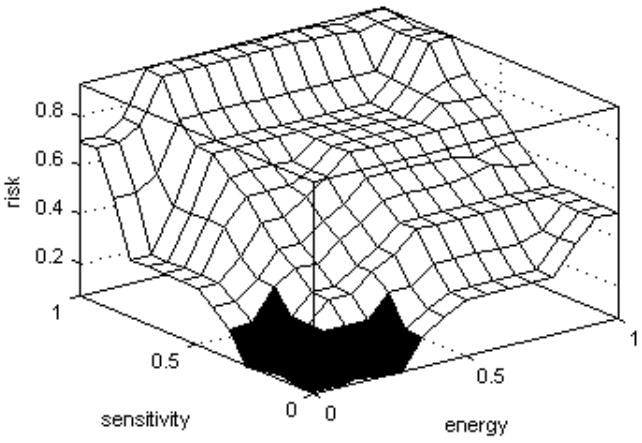

Figure 4. Surface view - input and output space relationship

6. Conclusion

AMI introduction is one of the most significant technological changes in the power system. However, installation of smart meters, introduces an unprecedented level of exposure to the power system components. Many of these aspects have not been addressed properly in the early stages of AMI development. Utilities are becoming increasingly aware of this issue and are looking for appropriate ways to perform risk analysis and plan for mitigation strategies. This paper proposed the application of Mamdani type fuzzy inference in modelling the risk of smart meter attack and takes into consideration customer sensitivity and consumption patterns. The

proposed model is flexible and can be extended to include other input variables and risk assessment criteria. Finally, it can be concluded that this area proves to be very interesting for future research. Some of the most important future research directions in IDS will include privacy concerns, data collection, and storage from the cost and security perspective and technology management models.

References

[1]. Anderson, R. & Fuloria, S. (2011). *Smart meter security: a survey*, University of Cambridge Computer Laboratory, UK, available at: https://www.cl.cam.ac.uk , [accessed 11. Jan 2018].

[2]. Anderson, R. & S, Fuloria, S. (2010). *On the security economics of electricity metering*, Workshop on the Economics of Information Security WEIS 2010

[3]. Faisal, M. A., Aung, Z., Williams, J. R., & Sanchez, A. (2012, May). Securing advanced metering infrastructure using intrusion detection system with data stream mining. In *Pacific-Asia Workshop on Intelligence and Security Informatics* (pp. 96-111). Springer, Berlin, Heidelberg.

[4]. Grochocki, D., Huh, J. H., Berthier, R., Bobba, R., Sanders, W. H., Cárdenas, A. A., & Jetcheva, J. G. (2012, November). AMI threats, intrusion detection requirements and deployment recommendations. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on* (pp. 395-400). IEEE.

[5]. Dickerson, J. E., Juslin, J., Koukousoula, O., & Dickerson, J. A. (2001, July). Fuzzy intrusion detection. In *Ifsa world congress and 20th nafips international conference, 2001. joint 9th* (Vol. 3, pp. 1506-1510). IEEE.

[6]. Pourfallah S., Jafari A.H., Shahhoseini H.S., Oleyaeyan M., (2014). An intrusion detection algorithm for AMI systems based on SVM and PC, *International Journal on Cybernetics & Informatics (IJCI)* Vol. 3, No. 4.

[7]. Vinchurkar D.P. & Reshamwala A., (2012). A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique, *International Journal of Engineering Science and Innovative Technology*, Volume 1, Issue 2.

[8]. Yao, J. T., Zhao, S. L., & Saxton, L. V. (2005, March). A study on fuzzy intrusion detection. In *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005* (Vol. 5812, pp. 23-31). International Society for Optics and Photonics.

[9]. Ahmad, S., & Baig, Z. (2012). Fuzzy-based optimization for effective detection of smart grid cyber-attacks. *Int. J. Smart Grid Clean Energy*, *1*(1), 15-21. DOI: 10.12720/sgce.1.1.15-21

[10]. Šarić, M. (2014, November). Fuzzy approach for evaluating risk of service interruption used as criteria in electricity distribution network planning. In *Neural Network Applications in Electrical Engineering (NEUREL), 2014 12th Symposium on*(pp. 79-84). IEEE.

[11]. Electric power research institute (EPRI), (2012). Intrusion Detection System for Advanced Metering Infrastructure" Technical report, available at: https://www.epri.com/#/pages/product/1026553/ [accessed 05. Jan 2018].

[12]. Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., & Shen, X. S. (2014). Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, *19*(2), 105-120.

[13]. McLaughlin, S., Podkuiko, D., & McDaniel, P. (2009, September). Energy theft in the advanced metering infrastructure. In *International Workshop on Critical Information Infrastructures Security* (pp. 176-187). Springer, Berlin, Heidelberg.

[14]. Bojadziev G., Bojadziev G., (2007). Advances in Fuzzy Systems: Applications and Theory"— 2nd edition, Vol. 23, *World Scientific Publishing Co. Pte. Ltd.*

[15]. Zhang, T., Zhang, G., Ma, J., & Lu, J. (2010). Power distribution system planning evaluation by a fuzzy multi-criteria group decision support system. *International Journal of Computational Intelligence Systems*, *3*(4), 474-485.

[16]. Lo, C. H., & Ansari, N. (2013). CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid. *IEEE Transactions on Emerging Topics in Computing*, *1*(1), 33-44.