


RESEARCH

Open Access



A rule-based model for electricity theft prevention in advanced metering infrastructure

Abdulrahman Okino Otuoze^{1,2*} , Mohd Wazir Mustafa¹, Abiodun Emmanuel Abioye³, Umbrin Sultana⁴, Ayinde Muhammed Usman², Oladimeji Ibrahim², Isaac Ozovehe Avazi Omeiza² and Abdallah Abu-Saeed⁵

*Correspondence:
oabdulrahman2@live.
utm.my

¹ Department of Electrical
Power Engineering, Universiti
Teknologi Malaysia, Johor
Bahru, Malaysia
Full list of author information
is available at the end of the
article

Abstract

The deployment of smart electricity meter (SEM) via the advanced metering infrastructure (AMI) has come under cyber-attacks as adversaries continue to exploit the communication links for possible evasion of electricity bill payments. Various detection models relying on energy consumption data offer a disadvantage of delayed detection and consequent huge financial losses before frauds are detected. Moreover, existing techniques mostly concentrate on detection of electricity thefts and rely on energy consumption data alone as the basis of theft perpetration whereas other potential parameters which could be exploited for electricity theft prevention exist in AMI. In this study, AMI parameters, which are indicative of electricity thefts are preselected and modelled for electricity theft prevention. First, a given AMI network is sectioned into zones with the selected parameters modelled to define security risks by formulated set of rules based on real-time scenarios. Fuzzy inference system is then employed to model the security risks to ascertain the compromised state of the monitored parameters at the defined scenarios. The result of the developed model at 50% weight of each of the modelled parameters with interdependencies show clear indications of the modelled parameters and their interactions in the determination of risks. The decisions on monitored parameters evaluated at every timestep reveal varied dense velocity behaviours for every scenario. The result is suitable for monitoring the AMI in reporting and/or disconnecting any compromised SEM within a considerable timestep before huge losses are incurred. Implementation of this scheme will contribute a significant success in the attempt to prevent electricity theft perpetration via the AMI.

Keywords: Advanced metering infrastructure, Electricity theft prevention, Fuzzy inference system, Smart electricity meters

Introduction

In the traditional systems, electricity theft is the main source of non-technical losses (NTL). They are carried out majorly by physical tampering of the meters, billing manipulations, poor revenue collection techniques, corrupt practices with internal staff usually involving lowering of bills, lack of accountability by the utility management, general commercial systems' inefficiencies, etc. [1–4]. The introduction of digital prepaid meters to address the inaccuracies associated with the conventional metering system is hindered by technical and operational issues [5–7] such as meter tampering, sales of fake or

unauthorized prepaid vouchers, and other corrupt practices. Fortunately, the advent of highly sophisticated measurement, control, communication, and high computing schemes which birthed a revolutionised grid system known as smart grids (SG) offer the introduction of smart electricity meters (SEM) through advanced metering infrastructure (AMI). SG necessitate a broad acquisition and analysis of data for efficient management and operations of power systems [8–10].

AMI offer efficient metering allowing a two-way interaction between the utility provider and the consumers. The capability of AMI to record and transmit real-time consumption data, real-time pricing, and flexible control commands have made the implementation of AMI a key aspect of SG. This lays a positive landmark for the mitigation of NTL [11]. The AMI help to curb physical meter tampering, meter theft, meter swapping, estimated billing irregularities, meter bypass, sales of fake prepaid vouchers [12–20], and other physical manipulations for electricity thefts. It is also equipped with improved protective measures offering intrusion monitoring for secured communication links [21]. However, a key security risk in the form of cyber-attacks poses daring challenges to the deployment of SEM in AMI despite its potential advantages as smart technologies continue to face cyber-attacks by adversaries. This is due to the vulnerability of the communication links exposing the system to attacks by adversaries by possible manipulations for various motives [22–26]. These vulnerabilities in AMI are reportedly being exploited for electricity thefts [12, 19, 27–30]. Where physical connections to the meter itself are manipulated in the conventional meters, SEM data are subject to manipulations by software-based attacks [27, 28, 31–36], etc. Thus, making the security of AMI a necessity for every utility.

Electricity thefts remain a major concern to the deployment of AMI as huge losses are reportedly incurred worldwide in addition to the increasing reports of cyber threats [28, 37]. Despite the relief presented by AMI, a new dimension of threats posing unique challenges to the detection of NTL necessitate the need for the development of robust techniques for a timely identification and elimination of threats [12, 28, 35]. Although the AMI is faced with increased threats, they provide adequate data from the installed sensors for useful analytics and inferences for various decision supports. Moreover, the monitoring of customers' consumption data and other control measures can be achieved via the AMI as it interconnects and communicates data with customers, utilities, and third parties [28, 38–42]. Reported algorithms utilizing energy consumption data are yet to substantially consider real-time monitoring of other parameters of the AMI which are indicative of electricity thefts. Moreover, existing approaches often consider a general practice of evaluating a common threshold for determining energy theft despite the stochasticity of individual consumption data. Therefore, the need for a consumer-based preventive model relying on the selection of real-time monitoring parameters which are indicative of electricity thefts. These parameters equally offer suitable decision support for a stochastic time-series data as those of SEM.

This work presents an electricity theft prevention scheme for the AMI utilizing electricity thefts' indicative parameters which are suitable for a real-time monitoring. The AMI network is sectioned into zones and each zone is effectively monitored based on defined compromised and uncompromised states scenarios. Security risks are defined for each of the scenarios and translated into rules which are further implemented using a

fuzzy inference system. Next, section II discusses the report of some related works while Section III presents the methodology of the model formulations. Section IV discusses the results of the developed model with implemented prevention scheme and section V concludes the study.

Related works

The securities of AMI have been a major concern particularly on the threats posed via cyber-attacks as have been demonstrated in many studies [19, 21, 43–52]. However, AMI offers a reliable and secured platform which are leveraged for curbing electricity thefts. This is achieved by its many interconnected sensors which make the SEM record zero reading and transmit same to utility system by utilizing the powerline communication medium [53]. The background of AMI and the major security requirements were discussed by Jiang [28] while presenting an attack model to describe energy theft behaviour aimed at timely detection of malicious activities. The study by Singh [54], Jiang [28], Mohassel [55], Jokar [56], Jokar [12] McLaughlin [57], Shekari [58], and many others reveal that AMI attacks are launched mostly at the communication channel to transmit falsified data which could be aimed at committing frauds. Consequently, the susceptibility of the AMI communication channel to cyber-attacks necessitated increased research in the cyber-related studies. Shuaib [41] posited how Denial of Service and Man-in-the-middle attacks could be exploited in local area network (LAN) to launch a cache of attacks to corrupt SEM via the address resolution protocol. These attacks could cripple the systems' functions by interrupting its communication with other network hosts. Once corrupted, these data represent false data which could be manipulated to cause evasion of bill payments and false estimated values of state variables [59–62]. Several studies revealed increased attention is being paid to ascertaining the impact on state estimations of measurements by grid sensors and how these injected attacks can be used to launch coordinated attacks [63–67].

Liu [68] examines how false data injection (FDI) attacks affect state estimations in power grid. He reported that intrusions could be observed from the sensors due to cyber-attacks but proposes the monitoring of the state estimates could help check intrusions. The state estimations of redundant sensor measurements and network topology information are used to determine the state of grid system and could also be adapted by appropriate modelling to detect malicious measurements [69]. The study by Lo and Ansari [70] presented a state-based estimation of grid sensor placement algorithm for a consumer attack model aimed at improving the intrusion detection accuracy and observability. Liang [67] in their studies, while highlighting the economic and physical impacts of emerging FDI attacks on modern power systems, discussed the basic approaches of launching a successful FDI attack with future directions hampering on improved security monitoring. Kallitsis [71] proposed an adaptive procedure to test data attack combined methods to avoid possible wrong grid-state estimates. Bi and Zhang [72] had attempted a prevention scheme to secure the state estimation from being compromised, by proposing a graph theoretic approach to construct an optimal set of meter measurements. Addressing the problem from a different angle, a semi-definite programming was

proposed by Su [73] to solve the state estimation problem for detecting and confirming electricity theft cases.

Khoo and Cheng [74] proposed a radio-frequency identification technology to detect the presence of malicious consumers' energy consumptions data for electricity theft prevention. Using an IoT scheme, Meanwhile, Xiao [75] developed a mutual inspection strategy for the discovery of compromised meters. In the study by McLaughlin et al. [76], an AMI intrusion detection utilising information fusion combining sensors' status and consumption data was proposed for energy theft detection. Atif [77] developed a multi-layered threat model and analysis based on evaluation metrics of cyber-physical systems' vulnerability. The study by Liu [78] demonstrated that electricity theft could be committed by exploiting the multiple pricing schemes offered by the AMI. The study analysed multiple pricing schemes and the related threats while proposing an attack model and countermeasures for enhanced protection. In another study, Ballal, Suryawanshi [79] proposed an online-based electricity theft prevention using programmable logic control to detect pilferage locations. However, the work is mainly directed at detecting direct tapping on the power lines. A periodicity analysis employing an autocorrelation function was performed to determine candidate periods from a Fast Fourier Transform-generated periodogram [80]. With the aid of selected machine learning models, the obtained result was further analysed for electricity theft detection. For SG application, theft must be prevented within the possible shortest time, but, time was not of key essence in the developed model. In a seemingly related approach, Jaiswal and Ballal [81] present a real-time electricity theft detection based on a fuzzy inference system to prevent hook-line activity on a power line. Nevertheless, traditionally, tampering is catered for in a typical SG, and therefore, does not require metering data to confirm. In another dimension, a penalization scheme for electricity thefts in AMI has been presented [82].

A lot of research works have been submitted bordering on the attempts to either detect or prevent electricity frauds but only a few are directed at AMI. Nonetheless, most works concentrate on utilization of the energy consumption profile while few other works are directed at building hardware systems for electricity theft prevention or detection. In addition, some of the presented techniques utilising state-based hardware designs are offered at extra costs and not suitable for a typical AMI network. Moreover, a breach of any of the identified security requirements or source of threats to AMI aimed at committing electricity thefts is manifested by known indications of thefts. The profile or the state of such indicators of electricity theft in AMI could be modelled for improved monitoring to aid necessary actions for the prevention of electricity thefts. The parameters, indicative of electricity thefts, have been discussed in [78, 83, 84] to include positive intrusion status, false signature on SEM data, erratic outage notification, de-energised or SEM outage, timestamp status, false pricing, flagged observer meter status, etc. Furthermore, they could be manifested in form of false estimation status, irregular or anomalous consumption profile, false timestamp, alteration of the billing information or false pricing regime, etc., depending on the intent of the attackers. Therefore, SEM are considered compromised depending on the inferences drawn based on the status of the monitored electricity thefts' indicative parameters which can be selected for modelling as presented in this research. Next

is the problem formulation of the adopted methodology for the proposed scenario-based modelling.

Methodology

To select the modelled parameters analysed in this work, a simplified AMI network is first presented. This simplified AMI network is considered analogous to the protection scheme of any given power systems. A number of consumers are connected to this network and then subdivided into protection zones. The zoning is achieved by grouping consumers in given locations with peculiar parameters modelled based on set rules to effectively help monitor and prevent electricity thefts in that zone. Then, an architecture for monitoring the consumers in each zone is developed. Four parameters indicative of electricity thefts are then selected and modelled with developed rules based on the defined states before being implemented using a fuzzy inference system (FIS).

Simplified AMI scheme for electricity thefts monitoring

In this scheme, SEM in a distribution network are considered segregated based on a neighbourhood comprising of different zones. Each zone represents a group of consumers while assuming the considerations of some arbitrary number of factors which include.

- Number of consumers in the neighbourhood under study.
- Type of consumers and their load consumption level.
- Intuitively estimated integrity of the consumers (based on previous electricity theft records).
- Ease of tracking and arresting of fraudulent consumers etc.

Figure 1 is the developed zones for a typical AMI monitoring of a neighbourhood network comprising n consumers. It is a random model which is not drawn to scale based on the factors mentioned above but basically to convey the segregation model. This sectioning will particularly offer the advantage of the ease of monitoring as the uncertainties are assumed to be reduced in such networks. In each of the identified zones, selected key

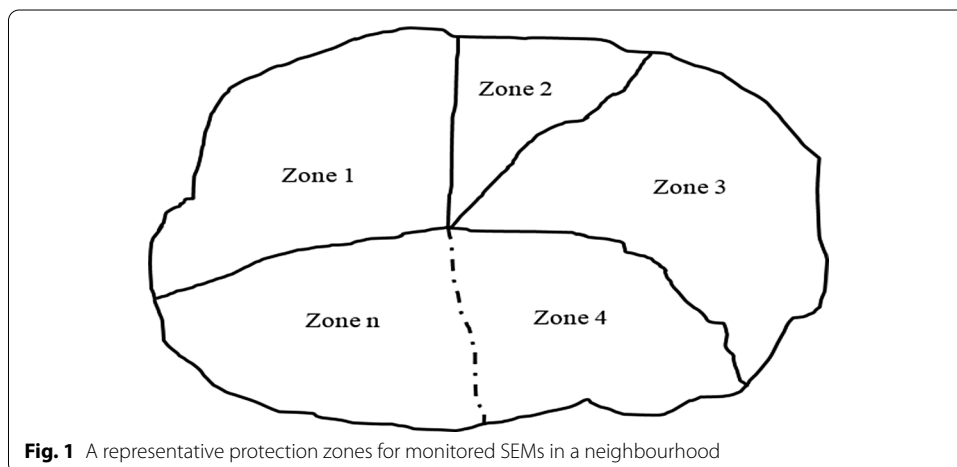
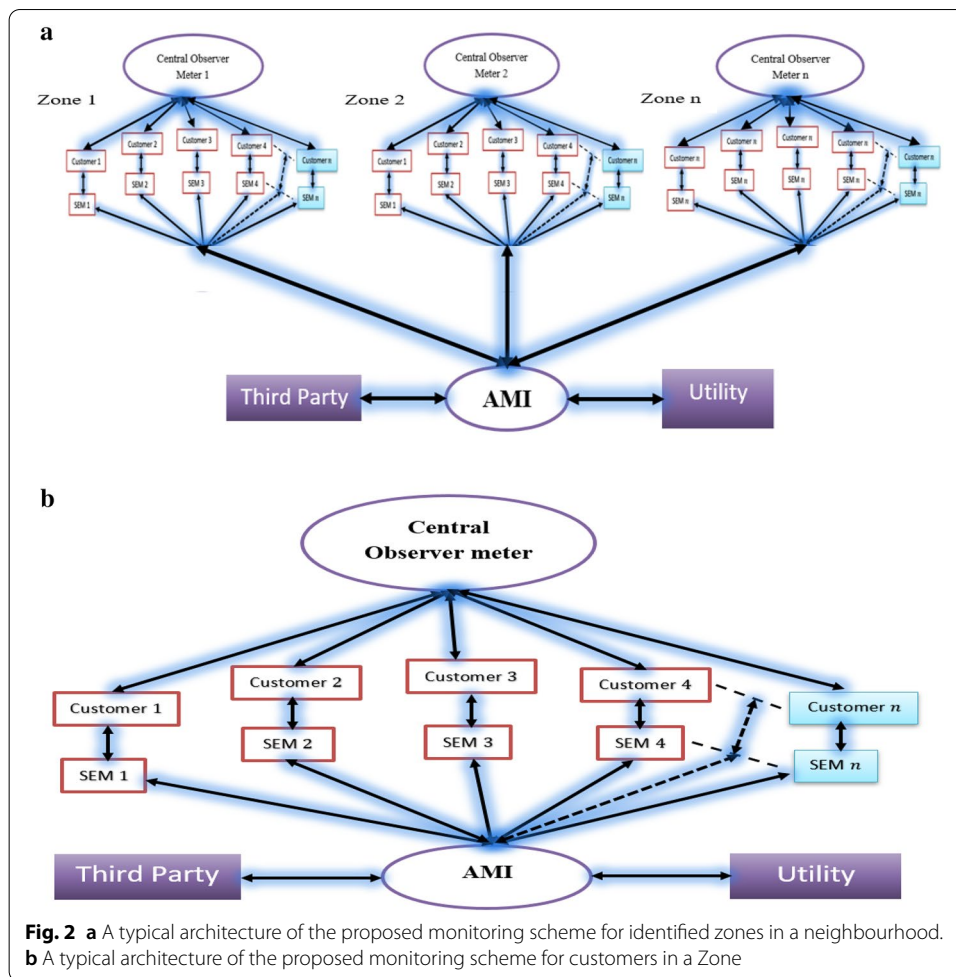


Fig. 1 A representative protection zones for monitored SEMs in a neighbourhood



network parameters of all the SEM are modelled for identification of possible compromise. Figure 2a represents the architecture of the proposed monitoring scheme in a protected zone. As shown in the figure, a central observer is connected to record the consumption of all SEM as well as monitor the respective protection zone. Furthermore, each consumer communicates with the AMI via the SEM. Figure 2b gives a clearer scenario of the proposed architecture for any given zone. Next, the parameters to be monitored are selected and modelled.

Selection and modelling of the monitored parameters

This study preselects the intrusion detection status of each zone (α), timestamp error of the SEM readings (β), real-time pricing error (γ), and the central observer meter status of each zone (δ) for monitoring. In this model, each compromised state is set to 'High' while the uncompromised state is set to 'Low'. The intrusion status, α is "High" when intrusion is detected and "Low" for cases of no intrusion at the given timestep. α is the direct output of the applied intrusion prevention or detection scheme being provided as in-built or additional mechanisms for primary protection of the SEM. First, the timestep (τ) is set as the period for which the states of all the monitored parameters are evaluated at timestamp (T) according to Eq. (1).

$$T_{\tau} - T_{\tau-1} = T_d \quad (1)$$

where T_{τ} is the timestamp at the current timestep of evaluation, $T_{\tau-1}$, the previous timestamp just before the current timestep of evaluation and T_d , the difference between the two timestamps. T_d must be constant at every timestep of evaluation for uncompromised states. Therefore, error is flagged when these values give inconsistent value of T_d . The timestamp error, β is evaluated using Eq. (2). β determines the error in the monitored timestamps and signals “High” for any inconsistency in the reported time interval within a given timestep and “Low” for normal timestamps.

$$\beta = \begin{cases} \text{Low, } \Delta T_d = 0 \\ \text{High, } \Delta T_d \neq 0 \end{cases} \quad (2)$$

γ represents the deviation from the set real-time pricing by the utility to what each SEM reflects. Let $p_{1,1}, p_{1,2}, p_{1,3}, \dots, p_{1,\tau}, p_{2,1}, p_{2,2}, p_{2,3}, \dots, p_{2,\tau}, p_{3,1}, p_{3,2}, p_{3,3}, \dots, p_{3,\tau}, \dots$; and $p_{n,1}, p_{n,2}, p_{n,3}, \dots, p_{n,\tau}$ be the instantaneous real-time pricing for customers 1, 2, 3 to n applied to the neighbourhood at timesteps 1, 2, 3 to τ , respectively. As presented in a previous work [83], the real-time pricing for each of the SEM can be authenticated based on Eqs. (3) to (5). Note that for a given neighbourhood, different pricing schemes may apply to different customers depending on the type of customers and other flexible service schemes available in the SG regime. However, in this work, Eq. (3) is formulated to ensure constant monitoring of the pricing regime among customers in a zone with the assumption that all customers in a zone are subjected to an equal tariff plan at any given timestep. Equation (3) shows that the state scenario of a customer’s pricing regime can be used as a check on other customers within the same zone. Equation (4) compares any given customer’s pricing regime with the set value by the utility at any τ where $p_{u,\tau}$ denotes the billing as set by the utility at timestep τ . To monitor deviation in the applied price regime to each of the customers’ SEM, Eq. (5) is formulated to define the state for both compromised and uncompromised states by constantly comparing the price regimes at utility and customer ends. When a customer’s pricing information is at equal state as the applied pricing by the utility, there is no suspected compromise, and the state “Low” is assumed, otherwise, the state “High” is assumed.

$$\sum_{\tau} p_{1,\tau} = \sum_{\tau} p_{2,\tau} = \sum_{\tau} p_{3,\tau} = \dots = \sum_{\tau} p_{n,\tau} \quad (3)$$

$$\sum_{\tau} p_{n,\tau} = \sum_{\tau} p_{u,\tau} \quad (4)$$

$$\gamma = \begin{cases} \text{Low, } p_{u,\tau} = p_{n,\tau} \\ \text{High, } p_{u,\tau} \neq p_{n,\tau} \end{cases} \quad (5)$$

The inclusion of the central observer meter as provided in Fig. 2 is to provide for a real-time monitoring of all SEM in the monitored zone to determine possible abnormal deviations. The deviations in the recorded energy consumption data of each of the SEM are modelled by comparing recorded values of the central observer meter with those of the SEM in a zone. At any given timestep, energy recorded by the observer meter, E_{Ob}

and the energy recorded by all SEM in the given zone, E_{SEM} , are monitored to determine possible compromise in each zone. Compromised or uncompromised state of the observer meter, δ , is modelled based on the value of k as given in Eq. (6) where k is the assumed maximum allowable unaccounted losses in a zone due to possible error in the estimation of technical losses (TL). This means the difference between the supplied energy to a zone and the reported consumption by all SEM must not be greater than k , in consideration of the TL for all uncompromised scenarios.

$$\delta = \begin{cases} \text{Low, } E_{Ob} - \sum E_{SEM} \leq k \\ \text{High, } E_{Ob} - \sum E_{SEM} > k \end{cases} \quad (6)$$

Defining the rules

Having selected and modelled the parameters to be monitored, the rules are then defined for the security risks based on all possible states for each of the parameters to enable efficient implementation of the monitoring scheme. To define the security risks, the following rules are formulated:

- i. A compromise of a monitored parameter does not translate to electricity theft as such could potentially be a false alarm, however, it is enough an important indicator of possible theft scenario.
- ii. A compromised parameter is defined to mean a “Low” security risk, two parameters for a “Medium” risk and compromise of all three parameters at a given scenario to mean a “High” security risk for α , β , and γ while a “Normal” security risk is defined when none of the parameters is reportedly compromised. Table 1 shows the defined set rules for the scenarios.
- iii. The observer meter status, δ , is set to highest priority over other monitored parameters. This is because any reflection of imbalance from the measurements of all the monitored SEM within the zone indicates a severe threat.

Using Eq. (4), Table 1 is then updated to Table 2 with δ where the state of other parameters remains unchanged when at state “Low” while other rules are as captured

Table 1 Defined rules for α , β , and γ scenarios, and the security risks

Scenarios	Defined rules for the security risk model			
	If			Then
	α	β	γ	Security risk
1	Low	Low	Low	Normal
2	Low	Low	High	Low
3	Low	High	Low	Low
4	Low	High	High	Medium
5	High	Low	Low	Low
6	High	Low	High	Medium
7	High	High	Low	Medium
8	High	High	High	High

Table 2 Updated rules for the scenarios of all the monitored parameters

Scenarios	Defined rules for the security risk model				
	If				Then
	α	β	γ	δ	Security risk
1	Low	Low	Low	Low	Normal
2	Low	Low	Low	High	Low
3	Low	Low	High	Low	Low
4	Low	Low	High	High	High
5	Low	High	Low	Low	Low
6	Low	High	Low	High	High
7	Low	High	High	Low	Medium
8	Low	High	High	High	High
9	High	Low	Low	Low	Low
10	High	Low	Low	High	High
11	High	Low	High	Low	Medium
12	High	Low	High	High	High
13	High	High	Low	Low	Medium
14	High	High	Low	High	High
15	High	High	High	Low	High
16	High	High	High	High	Very High

Table 3 Developed pseudocode for implementing the scenario model

Algorithm: Electricity theft prevention in AMI based on the selection of α , β , γ , and δ .

Input: T_τ , $T_{\tau-1}$, $p_{n,\tau}$, $p_{u,\tau}$, k , E_{Ob} , E_{SEM}

Output: α , β , γ , δ

check for intrusion detection status, α , timestamp error, β , real time pricing error, γ and observer meter status, δ ;

For $i = 1$ **to** τ ;

If no intrusion is detected, α is “Low”, Else α is “High”;

If $\Delta T_d = 0$, Then β is “Low” Else “High”;

If $p_{u,\tau} = p_{n,\tau}$ Then γ is “Low” Else “High”;

If $E_{Ob} - \sum E_{SEM} \leq k$ Then δ is “Low” Else “High”;

Do

 Security Risk \leftarrow Solve Table 2

Return α , β , γ , δ , Security risk

Next i

End if

End if

End if

End if

End

in Table 2. The status of all the monitored parameters by utilizing the set rules are achieved based on the developed pseudocode of Table 3. This is implemented using FIS.

Developed input–output model and the fuzzy sets for electricity theft prevention

The set rules and algorithm developed in Tables 2 and 3 are implemented by FIS using MATLAB R2019b. Figure 3 shows the developed input and output layout utilising the popular Mamdani model. The Mamdani model is chosen because it offers easier and

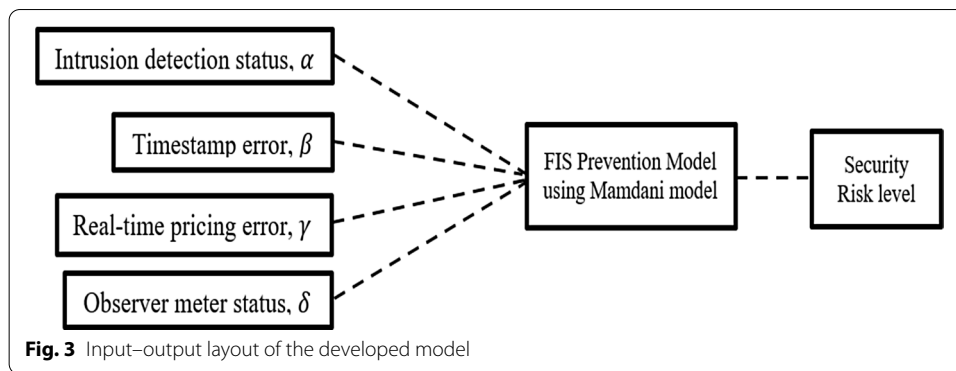


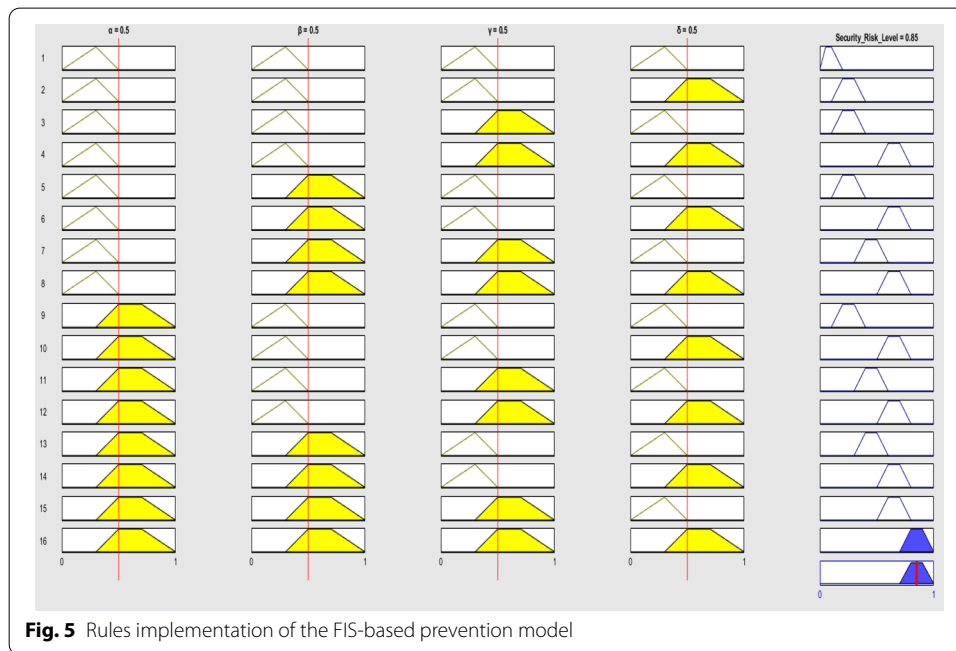
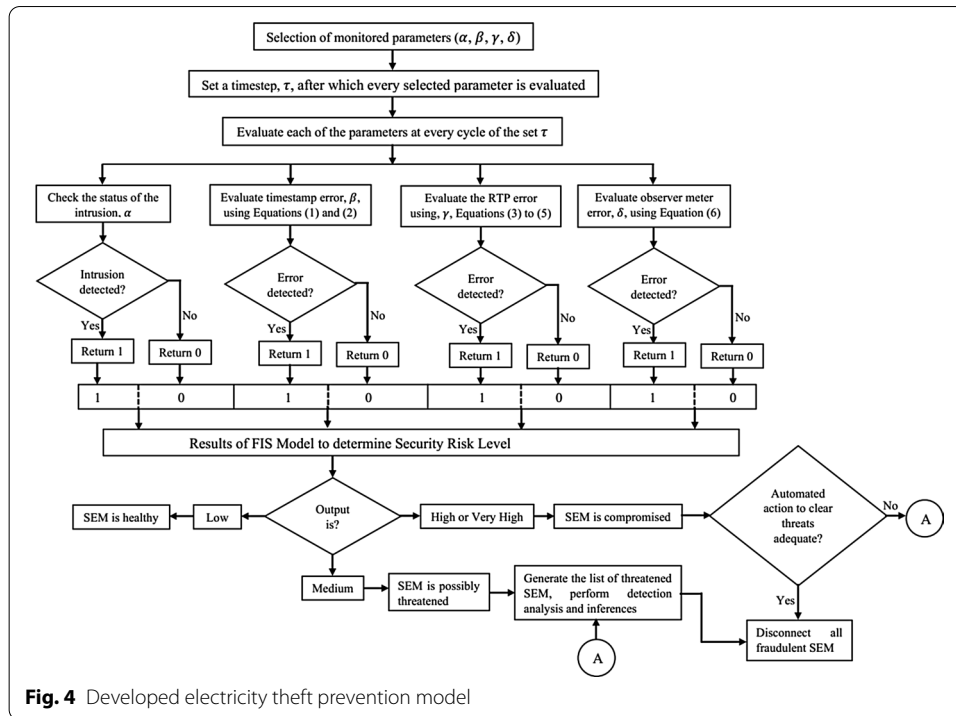
Table 4 Defined fuzzy sets for the input and output membership functions

Defined state level	Membership function	Fuzzy sets
<i>Input</i>		
Low	Triangular	[0 0.3 0.5]
High	Trapezoidal	[0.3 0.5 0.7 1]
<i>Output</i>		
Normal	Trapezoidal	[0 0.05 0.1 0.2]
Low	Trapezoidal	[0.1 0.2 0.3 0.4]
Medium	Trapezoidal	[0.3 0.4 0.5 0.6]
High	Trapezoidal	[0.5 0.6 0.7 0.8]
Very high	Trapezoidal	[0.7 0.8 0.9 1]

more instinctive implementation of rules as it is better suited for the development of expert systems based on expert knowledge as presented in this study. Triangular and trapezoidal membership functions were defined for the input “Low” and “High”, respectively. Although no specific membership function is prescribed for any event, every human-expert system requires a fundamental understanding and possibly some trial-and-error approach, as was followed in this model. Table 4 shows the fuzzy set defined for the input and output.

Developed electricity theft prevention model based on the implemented rules

The developed electricity theft prevention model implemented based on utilisation of the results of the FIS model for all modelled scenarios is given in Fig. 4. Decisions on monitored parameters are evaluated at every timestep and are firmly based on Fig. 4. If there is any risk (defined to be the “High” or “Very High” states), an attempt is made to automatically clear the threat before electricity theft is significantly committed. This adequately improves the self-healing function of the AMI. Such compromised state may necessitate further assessment or action to secure the system usually by subjecting compromised SEM to further analysis depending on if the self-healing is not able to restore the system. As shown in the developed model, further analysis may be required where automated action becomes inadequate to clear suspicious status.



Results and discussion

The result of the developed model is as given in Fig. 5 at 50% weight of each of the modelled parameters. The result is determined by the selecting a monitored parameter with interdependencies on at least, one other parameter with respect to the

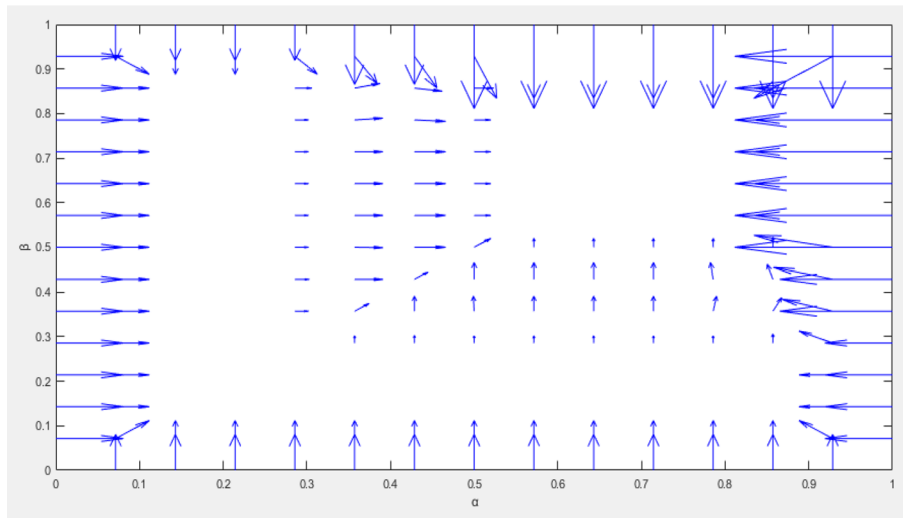


Fig. 6 Model dependency α and β on the security risk

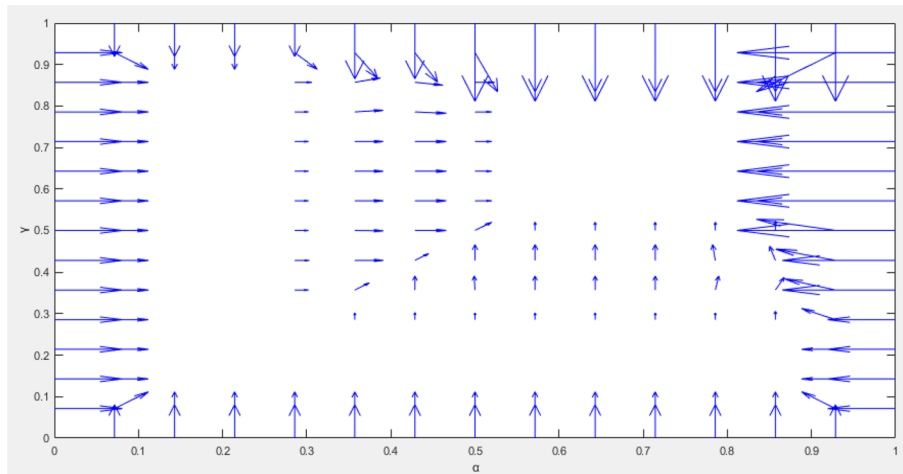


Fig. 7 Model dependency α and γ on the security risk

security level. These models are as shown in form of the velocity vectors of Fig. 6 through Fig. 11. Figures 6, 7 and 8 show that where observer meter reading error is not significant, threats are high, but covers densely in both dimensions with the observer meter error significant as replicated in Figs. 9, 10 and 11. These dense velocity behaviours depict the importance given to the state of the observer meter reading. The quiver or velocity plots give clear indications of the modelled parameters and their interactions in the determination of risks. Sometimes, errors could be due to a faulty sensor, and the output of the quiver plot comes in handy to help the operator make a desired decision. This evaluation is carried out at every set timestep, τ and is selected to be as short as to allow the prevention scheme to act before any significant loss is incurred in cases of compromise. τ is to be effectively determined by the utility. τ can be chosen to be as low as every minute but to allow for proper

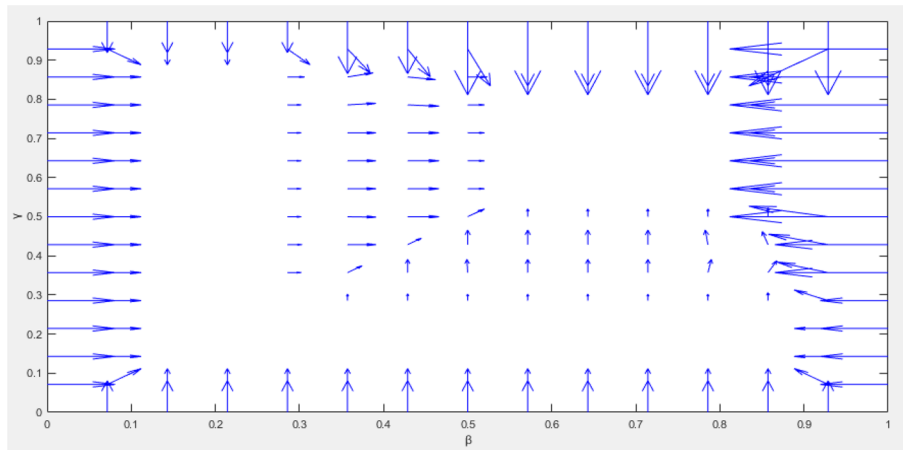


Fig. 8 Model dependency γ and β on the security risk

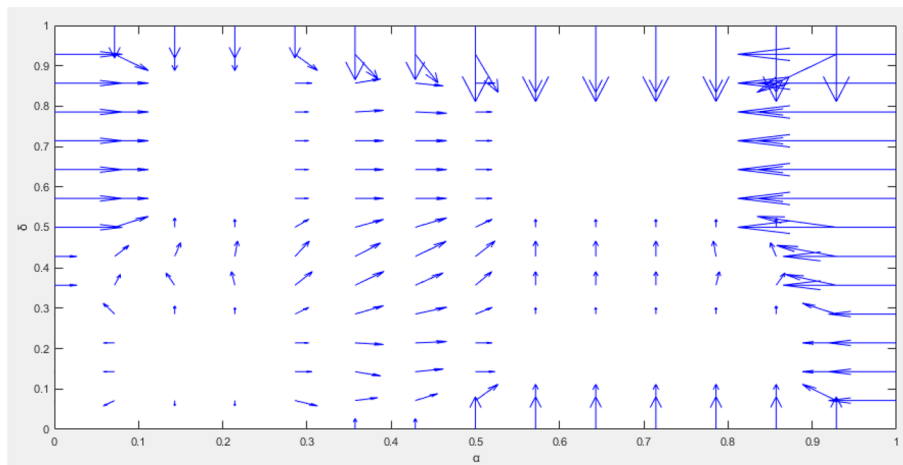


Fig. 9 Model dependency of δ and α security risk

and unexaggerated period of monitoring, it should be in a few hours cycle, although the choice of τ significantly depends on the operational planning of the utility. This scheme offers an improved level of security for a typical AMI. This work presents a new dimension in the studies of electricity theft prevention in AMI as this is the first approach of modelling selected electricity theft indicative parameters. The main contribution of this paper is the provision of enhanced monitoring measures for AMI to help prevent electricity theft. If implemented, the selected state parameters offer adequate enhancement on the security architecture of the AMI.

Conclusion

Prevention of electricity thefts in AMI is a key aspect of SG implementation. To prevent possible electricity theft in AMI, this study provided a novel rule-based design to model selected parameters indicative of electricity thefts. The parameters were modelled based on a set of rules for various scenarios to define security risks before applying a

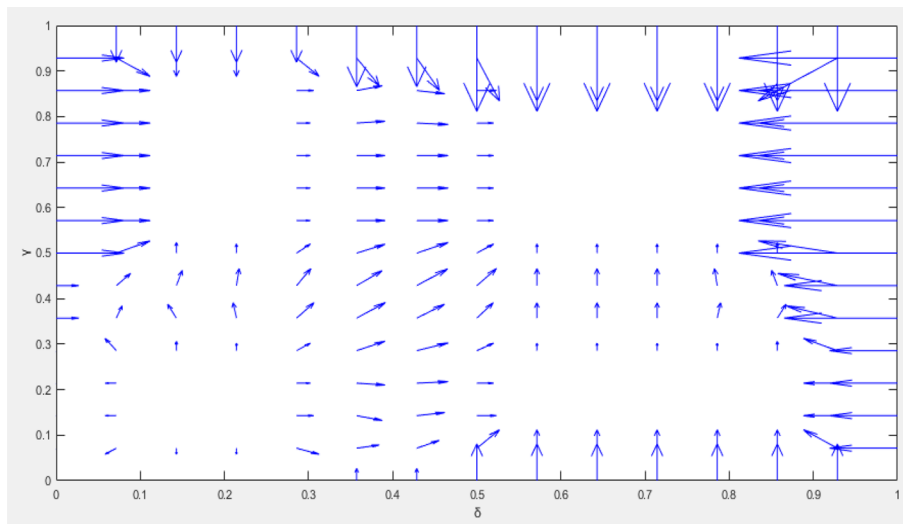


Fig. 10 Model dependency of δ and γ on the security risk

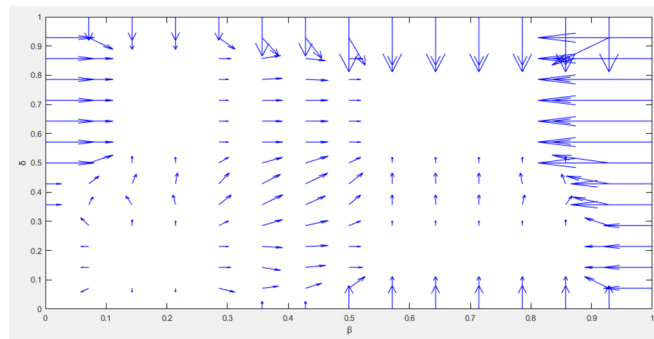


Fig. 11 Model dependency of δ and β on the security risk

rule-based technique utilizing FIS model. The results show that the monitored parameters allow for easy identification of compromised scenarios indicated by the dense area of the quiver plots. Enhancement in the monitoring scheme of AMI is achieved and serves as an additional layer to its security architecture. This scheme, implementable in smart utility networks, offers a simplified AMI with divisions into zones for ease of monitoring while providing increased security by monitoring selected and modelled parameters for prompt response in the prevention of electricity thefts. Further works may incorporate more indicative parameters to offer enhanced security and could also involve a real-time monitoring of the energy consumption. Artificial intelligence techniques could also be explored to develop enhanced robust techniques based on data from the installed sensors on AMI.

Abbreviations

AMI: Advanced metering infrastructure; FDI: False data injection; FIS: Fuzzy inference system; NTL: Non-technical losses; SEM: Smart electricity meter; SG: Smart grids.

Acknowledgements

The authors acknowledge the support of University Teknologi Malaysia and the University of Ilorin for the use of their facilities for this research work.

Authors' contributions

AOO developed the concept, participated in the design of the methodology, formal analysis, original draft preparation and writing, and investigation. MWM provided the resources, participated in the investigations, validation of the design, and was the project administrator. AEA participated in the writing of the original draft, validated the design using MATLAB resources, and involved in the formal analysis and writing of the results. US contributed to the writing of the review, the structure of the final version as well as editing, and supervision. AMU also participated in the design of the methodology, was involved in the formal analysis, and Writing of the review & editing. OI was involved in the original draft preparation, MATLAB design validation, and general review for enhanced comments. IOAO and AAS both supported the writing of the methodology, the general draft preparations, visualization of the results, and Writing—Review & Editing. All authors read and approved the final manuscript.

Funding

No funding was specifically received for this research.

Availability of data and materials

This work is based on 'states' using fuzzy set rules. So, data sharing does not apply.

Declarations

Competing interests

All Authors have read and approved the manuscript. I declare that none of the authors or any known person/body has any competing interest regarding this manuscript.

Author details

¹Department of Electrical Power Engineering, Universiti Teknologi Malaysia, Johor Bahru, Malaysia. ²Department of Electrical and Electronics Engineering, University of Ilorin, Ilorin, Nigeria. ³Department of Electrical/Electronic Engineering, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State, Nigeria. ⁴Department of Electrical Engineering, NED University of Engineering and Technology, Karachi, Pakistan. ⁵Department of Electrical/Electronic Engineering, Kogi State Polytechnic, Lokoja, Nigeria.

Received: 12 October 2021 Accepted: 26 January 2022

Published online: 16 February 2022

References

- Ahmad T, Ul Hasan Q (2016) Detection of frauds and other non-technical losses in power utilities using smart meters: a review. *Int J Emerg Electric Power Syst* 17(3):217–234
- Costa BC et al (2013) Fraud detection in electric power distribution networks using an ANN-based knowledge-discovery process. *Int J Artif Intell Appl* 4(6):17
- Nizar A, Dong Z (2009) Identification and detection of electricity customer behaviour irregularities. In: Power systems conference and exposition, 2009. PSCE'09. IEEE/PES. IEEE
- Agüero JR (2012) Improving the efficiency of power distribution systems through technical and non-technical losses reduction. In: Transmission and distribution conference and exposition (T&D), 2012 IEEE PES. IEEE
- Musungwini S (2016) A framework for monitoring electricity theft in Zimbabwe using mobile technologies. *J Syst Integr* 7(3):54
- de Souza Savian F et al (2021) Non-technical losses: a systematic contemporary article review. *Renew Sustain Energy Rev* 147:111205
- Aslam Z et al (2020) An attention guided semi-supervised learning mechanism to detect electricity frauds in the distribution systems. *IEEE Access* 8:221767–221782
- Alahakoon D, Yu X (2016) Smart electricity meter data intelligence for future energy systems: a survey. *IEEE Trans Inf Inf* 12(1):425–436
- Kulkarni V et al (2021) Power systems automation, communication, and information technologies for smart grid: a technical aspects review. *Telkomnika* 19(3):1017–1029
- Refaat SS et al (2021) Smart grid enabling technologies. Wiley
- Noufal K (2021) Autonomous authentication and light weight key management scheme for communication in smart metering infrastructure. *Turk J Comput Math Educ (TURCOMAT)* 12(10):1148–1156
- Jokar P, Arianpoo N, Leung VC (2016) Electricity theft detection in AMI using customers' consumption patterns. *IEEE Trans Smart Grid* 7(1):216–226
- Li H et al (2012) Efficient and secure wireless communications for advanced metering infrastructure in smart grids. *IEEE Trans Smart Grid* 3(3):1540–1551
- Lu B, Ma Y (2013) Research on communication system of advanced metering infrastructure for smart grid and its data security measures. *Power Syst Technol* 37(8):2244–2249
- Enbo J (2010) Smart meter system design in smart grid advanced metering infrastructure AMI. *Electr Meas Instrum* 47(7A):36–39
- Shahinzadeh H, Hasanizadeh-Khosroshahi A (2014) Implementation of smart metering systems: challenges and solutions. *TELKOMNIKA Indones J Electr Eng* 12(7):5104–5109

17. Anzalchi A, Sarwat A (2015) A survey on security assessment of metering infrastructure in smart grid systems. In: SoutheastCon 2015. IEEE
18. Otuoze AO et al (2019) Threats and challenges of smart grids deployments—a developing nations' perspective. *ELEKTRIKA-J Electr Eng* 18(2):33–43
19. Jokar P, Arianpoo N, Leung VC (2015) Electricity theft detection in AMI using customers' consumption patterns. *IEEE Trans Smart Grid* 7(1):216–226
20. Jokar P (2016) Detection of malicious activities against advanced metering infrastructure in smart grid. University of British Columbia
21. Mashima D, Cárdenas AA (2012) Evaluating electricity theft detectors in smart grid networks. In: International workshop on recent advances in intrusion detection. Springer
22. Otuoze AO, Mustafa MW, Larik RM (2018) Smart grids security challenges: classification by sources of threats. *J Electr Syst Inf Technol* 5(3):468–483
23. Olakanmi OO (2021) PASS: a privacy-aware approach for secure smart metering in advanced metering infrastructure networks. *J Appl Secur Res* 16(1):37–62
24. Singh NK, Mahajan V (2021) End-user privacy protection scheme from cyber intrusion in smart grid advanced metering infrastructure. *Int J Crit Infrastruct Prot* 34:100410
25. England BS, Alouani AT (2021) Internet-based advanced metering and control infrastructure of smart grid. *Electr Eng* 103(6):2989–2996
26. Clements S, Kirkham H (2010) Cyber-security considerations for the smart grid. In: IEEE PES general meeting. IEEE
27. Anas M et al (2012) Minimizing electricity theft using smart meters in AMI. In: 2012 Seventh international conference on P2P, parallel, grid, cloud and internet computing. IEEE
28. Jiang R et al (2014) Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Sci Technol* 19(2):105–120
29. Kimani K, Oduol V, Langat K (2019) Cyber security challenges for IoT-based smart grid networks. *Int J Crit Infrastruct Prot* 25:36–49
30. Krishna VB et al (2016) F-DETA: A framework for detecting electricity theft attacks in smart grids. In: 2016 46th Annual IEEE/IFIP international conference on dependable systems and networks (DSN). IEEE
31. Kakran S, Chanana S (2018) Smart operations of smart grids integrated with distributed generation: a review. *Renew Sustain Energy Rev* 81:524–535
32. Gunduz MZ, Das R (2018) Analysis of cyber-attacks on smart grid applications. In: 2018 International conference on artificial intelligence and data processing (IDAP). IEEE
33. Siboni S, Cohen A (2015) Universal anomaly detection: algorithms and applications. arXiv preprint <http://arxiv.org/abs/1508.03687>
34. Erol-Kantarci M, Mouftah HT (2013) Smart grid forensic science: applications, challenges, and open issues. *IEEE Commun Mag* 51(1):68–74
35. Sun C-C, Liu C-C, Xie J (2016) Cyber-physical system security of a power grid: State-of-the-art. *Electronics* 5(3):40
36. De Dutta S, Prasad R (2019) Security for smart grid in 5G and beyond networks. *Wirel Pers Commun* 106(1):261–273
37. Sharma T et al (2016) Of pilferers and poachers: combating electricity theft in India. *Energy Res Soc Sci* 11:40–52
38. Siano P (2014) Demand response and smart grids—a survey. *Renew Sustain Energy Rev* 30:461–478
39. Geelen D, Reinders A, Keyson D (2013) Empowering the end-user in smart grids: recommendations for the design of products and services. *Energy Policy* 61:151–161
40. Jokar P (2015) Detection of malicious activities against advanced metering infrastructure in smart grid. University of British Columbia
41. Shuaib K et al (2015) Resiliency of smart power meters to common security attacks. *Procedia Comput Sci* 52:145–152
42. Dong S, Cao J, Fan Z (2021) A review on cybersecurity in smart local energy systems: requirements, challenges, and standards. arXiv preprint <http://arxiv.org/abs/2108.08089>
43. Shein R (2010) Security measures for advanced metering infrastructure components. In: 2010 Asia-Pacific power and energy engineering conference. IEEE
44. Liu X et al (2015) A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. *IEEE Trans Smart Grid* 6(5):2435–2443
45. Wan Z et al (2014) SKM: scalable key management for advanced metering infrastructure in smart grids. *IEEE Trans Ind Electron* 61(12):7055–7066
46. Faisal MA et al (2012) Securing advanced metering infrastructure using intrusion detection system with data stream mining. In: Pacific-Asia workshop on intelligence and security informatics. Springer
47. Yan Y et al (2013) An efficient security protocol for advanced metering infrastructure in smart grid. *IEEE Netw* 27(4):64–71
48. Yao J et al (2017) Network topology risk assessment of stealthy cyber attacks on advanced metering infrastructure networks. In: 2017 51st Annual conference on information sciences and systems (CISS). IEEE
49. Guo Y et al (2015) Preventive maintenance for advanced metering infrastructure against malware propagation. *IEEE Trans Smart Grid* 7(3):1314–1328
50. Halle P, Shiyamala S (2021) SRAMI: secure and reliable advanced metering infrastructure protocol for smart grid
51. Wang B et al (2020) Research on data security of multicast transmission based on certificateless multi-recipient signcryption in AMI. *Int J Electr Power Energy Syst* 121:106123
52. Bhatt T, Kotwal C, Chaubey N (2019) Implementing AMI network using riverbed OPNET modeler for DDoS attack. *Int J Comput Sci Eng* 7(2):569–574
53. Luka MK, Olowononi F, Soja JS (2016) Power line communications: a platform for sustainable development. <http://eprints.covenantuniversity.edu.ng/6630/#.YgLgAmjMLDc>. Accessed 15 Aug 2021
54. Singh SK, Bose R, Joshi A (2018) Energy theft detection in advanced metering infrastructure. In: 2018 IEEE 4th world forum on internet of things (WF-IoT). IEEE
55. Mohassel RR et al (2014) A survey on advanced metering infrastructure. *Int J Electr Power Energy Syst* 63:473–484

56. Jokar P, Arianpoo N, Leung VC (2013) Intrusion detection in advanced metering infrastructure based on consumption pattern. In: 2013 IEEE international conference on communications (ICC). IEEE
57. McLaughlin S, Podkuiko D, McDaniel P (2009) Energy theft in the advanced metering infrastructure. In: International workshop on critical information infrastructures security. Springer
58. Shekari T (2021) Methods to attack and secure the power grids and energy markets. Georgia Institute of Technology
59. Nejabatkhah F et al (2021) Cyber-security of smart microgrids: a survey. *Energies* 14(1):27
60. Zhang H, Liu B, Wu H (2021) Smart grid cyber-physical attack and defense: a review. *IEEE Access* 9:29641–29659
61. TRAN N (2020) Design of false data injection (FDI) attacks against smart grid state estimation and FDI database generation. Australian Defence Force Academy
62. Aoufi S, Derhab A, Guerroumi M (2020) Survey of false data injection in smart power grid: attacks, countermeasures and challenges. *J Inf Secur Appl* 54:102518
63. Tao J, Michailidis G (2019) A statistical framework for detecting electricity theft activities in smart grid distribution networks. *IEEE J Sel Areas Commun* 38(1):205–216
64. Manandhar K et al (2014) Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans Control Netw Syst* 1(4):370–379
65. Yu Z-H, Chin W-L (2015) Blind false data injection attack using PCA approximation method in smart grid. *IEEE Trans Smart Grid* 6(3):1219–1226
66. Huang Y et al (2013) Bad data injection in smart grid: attack and defense mechanisms. *IEEE Commun Mag* 51(1):27–33
67. Liang G et al (2016) A review of false data injection attacks against modern power systems. *IEEE Trans Smart Grid* 8(4):1630–1638
68. Liu Y, Ning P, Reiter MK (2011) False data injection attacks against state estimation in electric power grids. *ACM Trans Inf Syst Secur (TISSEC)* 14(1):13
69. Bobba RB et al (2010) Detecting false data injection attacks on dc state estimation. In: Preprints of the first workshop on secure control systems, CPSWEEK
70. Lo C-H, Ansari N (2013) CONSUMER: a novel hybrid intrusion detection system for distribution networks in smart grid. *IEEE Trans Emerg Top Comput* 1(1):33–44
71. Kallitsis MG et al (2016) Adaptive statistical detection of false data injection attacks in smart grids. In: 2016 IEEE global conference on signal and information processing (GlobalSIP). IEEE
72. Bi S, Zhang YJ (2014) Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Trans Smart Grid* 5(3):1216–1227
73. Su C-L, Lee W-H, Wen C-K (2016) Electricity theft detection in low voltage networks with smart meters using state estimation. In: 2016 IEEE international conference on industrial technology (ICIT). IEEE
74. Khoo B, Cheng Y (2011) Using RFID for anti-theft in a Chinese electrical supply company: a cost-benefit analysis. In 2011 Wireless telecommunications symposium (WTS). IEEE
75. Xiao Z, Xiao Y, Du DH-C (2013) Non-repudiation in neighborhood area networks for smart grid. *IEEE Commun Mag* 51(1):18–26
76. McLaughlin S et al (2013) A multi-sensor energy theft detection framework for advanced metering infrastructures. *IEEE J Sel Areas Commun* 31(7):1319–1330
77. Atif Y et al (2018) Cyber-threat analysis for cyber-physical systems. University of Skövde
78. Liu Y et al (2020) Hidden electricity theft by exploiting multiple-pricing scheme in smart grids. *IEEE Trans Inf Forensics Secur* 15:2453–2468
79. Ballal MS et al (2020) Online electricity theft detection and prevention scheme for smart cities. *IET Smart Cities* 2(3):155–164
80. Ayogu II, Ogu RE (2021) An exploratory study of periodicity detection algorithms for energy theft prevention in smart grids. In: 2021 IEEE PES/IAS PowerAfrica. IEEE
81. Jaiswal S, Ballal MS (2020) Fuzzy inference based electricity theft prevention system to restrict direct tapping over distribution line. *J Electr Eng Technol* 15(3):1095–1106
82. Otuoze AO et al (2020) Penalization of electricity thefts in smart utility networks by a cost estimation-based forced corrective measure. *Energy Policy* 143:111553
83. Otuoze AO et al (2019) Electricity theft detection by sources of threats for smart city planning. *IET Smart Cities* 1(2):52–60
84. Jindal A et al (2020) Tackling energy theft in smart grids through data-driven analysis. In: 2020 International conference on computing, networking and communications (ICNC). IEEE