ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

AMI Mesh Networks Based Home Energy Management System

G.KausalyaDevi[1], M.Premkumar[2]

M.E, Applied Electronics, Sri Subramanya College Of Engineering And Technology, palani[1, 2]

Abstract: Advanced Metering is expected to be an integral part of energy grid. This paper describes a practical mesh networking solution based on extensions proposed to the routing protocol for low power and lossy networks (RPL) to realize automated metering communications. Advanced Metering Infrastructure (AMI) is the way of electricity is measured, consumed and even distributed. Power scheduling is achieved in home area network by power sharing and management. Mesh topology is used to form the home area network. Here we study the impact of the algorithms on the network discovery latency, recovery latency, and packet delivery ratio. Here we propose an efficient scheduling method for home power usage.

Index Terms: AMI, Mesh networks, Power scheduling, Performance.

I. INTRODUCTION

The Advanced Metering Infrastructure (AMI) is changing the way electricity is measured, consumed, and even distributed. Digital smart meters remotely report not only fine-grained energy consumption data, but also logs of events indicating malfunctions, misconfigurations, and potential physical tampering. These monitoring capabilities, coupled with large-scale AMI data aggregation promise to significantly mitigate the problem of energy theft, an especially pervasive problem in developing countries. AMI significantly increases the attack surface that utilities have to protect by introducing new cyber threats on physically-accessible devices. Automated metering is expected to be an integral part of the modern energy grid. Automated metering entails transport of metering data from the energy consumer's premises to the data management systems of the energy provider and potentially information in the other direction. Global energy generation and delivery systems are transitioning to a new computerized "smart grid". One of the principle components of the smart grid is an advanced metering infrastructure (AMI). AMI replaces the analog meters with computerized systems that report usage over digital communication interfaces, e.g., phone lines.

With the development of smart grid, residents have the opportunity to schedule their power usage in the home by themselves for the purpose of reducing electricity expense. We first introduce a general architecture of energy management system (EMS) in a home area network (HAN) based on the smart grid and then propose an efficient scheduling method for home power usage.

A variety of techniques have been discovered and performed to steal energy, starting from customer homes and up to the utility billing system. At the level of customer homes, the most common techniques are to tap energy from a neighbor or from a feeder or to tamper with meters so that consumption values are not properly recorded or not correctly reported. Tampering with meters includes applying magnets to slow down electromagnetic meters or to even pertubate measurements from solid state1 meters, reversing or disconnecting meters, and hacking into the firmware of smart meters. At the level of the grid, energy thefts usually bypass meters by wiring heavy appliances (e.g., AC or heater unit) directly to the grid, or connecting their entire electric system to a feeder with a pirate transformer. Finally at the level of the utility, intentional or unintentional inaccuracy in the billing system can cause important losses of energy revenue. Those inaccuracies are either unintentional (e.g., incorrect meter multiplier value to compute overall energy consumption from sample recording) or

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

intentional (e.g., customers switching their meter with a vacant premise or corrupted employees altering billing records). It is important to also note that the addition of smart communication infrastructure to the grid can increase attack vectors.

AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbours and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbours periodically its whole routing table. So they can check if there is a useful route to another node using this neighbour as next hop. When a link breaks a Count-To- Infinity could happen. AODV is an 'on demand routing protocol' with small delay. That means that routes are only established when needed to reduce traffic overhead. AODV supports Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently.

II. RELATED WORKS

A variety of techniques have been discovered and performed to steal energy, starting from customer homes and up to the utility billing system. At the level of customer homes, the most common techniques are to tap energy from a neighbor or from a feeder or to tamper with meters so that consumption values are not properly recorded or not correctly reported. Tampering with meters includes applying magnets to slow down electromagnetic meters or to even pertubate measurements from solid state1 meters, reversing or disconnecting meters, and hacking into the firmware of smart meters [4]. At the level of the grid, energy theft usually bypass meters by wiring heavy appliances (e.g., AC or heater unit) directly to the grid, or connecting their entire electric system to a feeder with a pirate transformer. Finally at the level of the utility, intentional or unintentional inaccuracy in the billing system can cause important losses of energy revenue. Those inacurracies are either unintentional (e.g., incorrect meter multiplier value alarms can never reach the utility database. Energy theft has been a problem for utilities since the
beginning of energy billing. Addressing this issue has been one of the motivation to invest in AMI [2], [5]. Indeed, smart meters have been designed to detect and report tampering attempts and the fact that they are solid-state eliminates some attack techniques that were popular with traditional analog meters. Alarms from smart meters have the potentialto identify meters being tilted, disconnected, reversed or even hacked into. In addition to invidual meter alarms, utilities can detect energy theft with higher accuracy by leveraging the large scope and detailed resolution of AMI data to correlate events over time and across their entire customer base with additional information [6], [7]. For example, utilities can be alerted about typical symptoms of energy theft such as
irregular outage notifications from a specific customer, or invalid consumption values from vacant premises. Moreover, detailed energy consumption profiles can be built over several months and change detection algorithms are applied to detect abnormal deviations (typically, a 20% threshold is used to trigger an alarm). Those profiles can be further normalized against customer profiles (e.g., residential or industrial) or geographical information system (GIS) so that outliers are easier to identify. Additionally, utilities can deploy meters on feeders or transformers to compare energy consumptions at the neighborhood level and at the level of individual meters.
Mismatches between values reported that cannot be justified by technical losses are used to trigger alerts.
While the wide array of detection techniques brought by AMI seems to offer a comprehensive solution, the problem of energy theft remains a critical issue and utilities are now facing two new important challenges. First, smart meters are actually not tamper-proof and [4], [8] even demonstrate that the deployment of AMI introduces a significant set of new attack techniques to achieve energy theft. Those techniques include interrupting measurements, gaining privileged access to the meter firmware, tampering with the meter storage, and intercepting the meter communications to block or alter consumption values being reported. Second, alarms from the
various energy theft detection techniques offered by AMI are highly prone to false positives (it is believed that up to 95% of tamper flags are erroneous [9]) and utilities now have the difficult new task of dealing with a deluge of data from which

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

identifying energy theft has become a sophisticated data mining challenge. Solutions to energy theft have also been introduced from academia over the past few years [10]. A popular approach has been to apply support-vector machine (SVM) to energy consumption profiles [11], [12]. This approach consists it raining a SVM from a historical dataset and then testing the SVM on a different dataset to find irregularities or deviations in the customer energy consumption profile. [11] reports an accuracy of 98.4% based on a training set of 440 instances and a testing set of 220 customers. The same authors extended their approach in [13] to leverage a hybrid neural-network model and encoding technique in order to automatically set the numerous parameters required by the SVM model. [14] studies a different method by focusing on identifying problematic metering installations (e.g., due to misconfiguration, energy theft or failure) through a central observer meter deployed at each neighborhood. This approach consists in comparing overall energy use with individual customer meters using a model of N linearly independent equations. This model is solved using matrix inversion and recursive statistical methods (i.e., least squares). The main limitations of this approach are to rely on a set of assumptions that often do not hold, such as the linear independence of equations or the zero resistance of energy cables. [15] takes a radically different approach by using a harmonic generator to actively deteriorate appliances of customers who steal energy. The concept is to monitor consumption values from smart meters, identify suspicious non-technical losses, disconnect genuine customers, operate the harmonic generator for few seconds and then reconnect everyone. An important limitation of this solution is to require smart meters to be instrumented with harmonic sensors so that genuine appliances remains protected from the active probes. Moreover, if such sensor fails, damage to genuine customers could make the cost of false positives prohibitively high.

III. PRELIMINARIES

A. Advanced Metering Infrastructure

The Advanced Metering Infrastructure (AMI) is changing the way electricity is measured, consumed, and even distributed. Digital smart meters remotely report not only fine-grained energy consumption data, but also logs of events indicating malfunctions, misconfigurations, and potential physical tampering. These monitoring capabilities, coupled with large-scale AMI data aggregation promise to significantly mitigate the problem of energy theft, an especially pervasive problem in developing countries.

As a result, the need for an efficient monitoring solution to detect energy theft attempts in AMI has never been more critical. In this paper, we introduce AMIDS, an integrated cyber-physical intrusion detection system to identify malicious energy theft attempts. AMIDS differs from previous solutions by evaluating multiple AMI data sources under a combination of techniques to detect theft-related behavior while reducing false positives. In particular, AMIDS uses an attack graph based information fusion technique to conceptually combine collected evidences from three types of AMI-specific information sources: 1) cyber-side network- and host-based intrusion detection systems; 2) on-meter anti-tampering sensors; and 3) power measurement-based anomalous consumption detectors through nonintrusive load monitoring (NILM). The main contributions of this paper are as follows:

• We present an information fusion solution which makes use of an AMI-specific attack graph to identify energy theft attempts with minimum number of false positives.

• We leverage data mining techniques to identify energy theft through nonintrusive load monitoring. We designed two algorithms: a supervised approach that can identify individual appliance consumption and an unsupervised approach that learns by clustering load events.

• We build a realistic household load simulator that we used to evaluate the different individual detection techniques and the information fusion solution through the injection of realistic energy theft attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

B. AODV Routing Protocol

The Ad-hoc On-demand Distance Vector (AODV) routing protocol is a routing protocol used for dynamic wireless networks where nodes can enter and leave the network at will. To find a route to a particular destination node, the source node broadcasts a RREQ to its immediate neighbors. If one of these neighbors has a route to the destination, then it replies back with a RREP. Otherwise the neighbors in turn rebroadcast the request. This continues until the RREQ hits the final destination or a node with a route to the destination. At that point a chain of RREP messages is sent back and the original source node finally has a route to the destination. We proved that AODV protocol never produces routing loops by proving that a combination of sequence numbers and hop counts is monotonic along a route. This means that there can't be any loop in the routing table. The proof was done completely automatically and our algorithm was able to generate all the predicates needed.

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. It is jointly developed in Nokia Research Center, University of California, Santa Barbara and University of Cincinnati by C. Perkins, E. Belding-Royer and S. Das. For other alternatives see the Ad hoc routing protocols list.

In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats.

Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

C. Power Scheduling Algorithm

Due to limited battery life of many mobile and embedded systems, power consumption is an important factor for any processing in these systems Power issue can be addressed in

- Architecture level
- System level
- Application level

Here the scheduling algorithms used are,

- Real Time Scheduling
- Hard Real Time
- Soft Real time
- Firm Real Time

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Context Switching in Scheduling

- Context switch time is the time taken to switch between two processes or threads in a schedule.
- The context switch duration is a hidden, unproductive duration in a schedule.
- The context switch duration includes the time taken for saving the context of the current process/ thread and loading the context of the next process / thread.

Where S is a 128 × 32 scrambling matrix. s is a number between 1 and 32. While building the matrix we make sure that the following conditions are met:
• The same row must not contain duplicate elements
• Rows must not be duplicates.
The detailed block diagram for the data embedding process is shown in Fig 4.3.

IV. PROPOSED WORK

The advanced Metering Infrastructure (AMI) is changing the way electricity is measured, consumed, and even distributed. Digital smart meters remotely report not only fine-grained energy consumption data, but also logs of events indicating malfunctions, misconfigurations, and potential physical tampering. These monitoring capabilities, coupled with large-scale AMI data aggregation promise to significantly mitigate the problem of energy theft, an especially pervasive problem in developing countries.

As a result, the need for an efficient monitoring solution to detect energy theft attempts in AMI has never been more critical. In this paper, we introduce AMIDS, an integrated cyber-physical intrusion detection system to identify malicious energy theft attempts. AMIDS differs from previous solutions by evaluating multiple AMI data sources under a combination of techniques to detect theft-related behavior while reducing false positives. In particular, AMIDS uses an attack graph based information fusion technique to conceptually combine collected evidences from three types of AMI-specific information sources: 1) cyber-side network- and host-based intrusion detection systems; 2) on-meter anti-tampering sensors; and 3) power measurement-based anomalous consumption detectors through nonintrusive load monitoring (NILM). The main contributions of this paper are as follows:

• We present an information fusion solution which makes use of an AMI-specific attack graph to identify energy theft attempts with minimum number of false positives.

• We leverage data mining techniques to identify energy theft through nonintrusive load monitoring. We designed two algorithms: a supervised approach that can identify individual appliance consumption and an unsupervised approach that learns by clustering load events.

• We build a realistic household load simulator that we used to evaluate the different individual detection techniques and the information fusion solution through the injection of realistic energy theft attacks.

Simulation Algorithm

Node Creation:

- Each home is considered as a node.
- Each node having sub-nodes referred as home electrical appliances.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- Set properties like queue length, location, protocols, routing algorithms
- Admin section (EB node) controls the entire set-up.

Link Establishment:

- Set types of link –Duplex, wireless, bandwidth, latency etc.
- Network Animator is a visual aid showing how packets flow along the network.
- AODV protocol is used for the control of the entire communication.

Power Scheduling:

High Power:

- Power is mutually supplied to all devices at each home.

Low Power:

- Power will be supplied only to particular devices at each home, which is set as a default in earlier represented by changing the color of appropriate devices (nodes).

V. PERFORMANCE

We also conducted performance evaluation of how long two major AMIDS analysis phases take to complete. First, we measured the time requirements for learning phases for profiling different households' electricity consumption patterns given the collected dataset of the smart meter measurements. It illustrates the results for smart meter measurement datasets of different time interval lengths. For instance, if the dataset stores the reported power measurements for a month (43200 minutes), AMIDS takes approximately 44 seconds to complete the dataset parsing, analysis, and household consumption profiling procedures. As expected, the analysis time grows linearly with the meter measurement dataset size. Although the learning phase is performed as an offline onetime effort, it is still important to complete the learning phase sufficiently fast for each household especially if a single power utility server is in charge of performing the analyses for many meters. Second, we evaluated the run time operation of the HMM-based energy theft detection component in AMIDS. In particular, we generated random attack graphs with different sizes (number of vertices) and a single attack path for each of them. Each attack path's length was equal to the graph's size. Then, we measured how long the HMM-based inference algorithm takes to start and complete the analyses, i.e., to report the best attack path estimate given the sensor alert sequence for the corresponding attack path.

AMIDS employs alerts triggered by different types of AMI sensors as well as Markovian information fusion techniques to identify malicious energy theft efforts effectively. However, AMIDS's large-scale deployment requires a few other capabilities and solutions to be in place. In the following, we review these requirements and limitations briefly. The in depth analysis of those requirements and their corresponding solutions are out of this paper's scope. As one of the energy theft detection algorithms, AMIDS employs the power measurements to perform a non-intrusive load monitoring and obtain information about what home appliances are being used in a particular household. Traditionally, usage of the NILM techniques in AMI infrastructures raises the concerns regarding customer privacy violations. The privacy violation concern in AMIDS can be addressed through two major techniques potentially. First, AMIDS can employ only the unsupervised learning-based techniques that do not distinguish individual home appliances by fingerprinting their electricity consumption signatures. Clearly, ignoring the extra information from the supervised solution will affect the energy theft detection accuracy of the AMIDS framework. Alternatively, as the more technical solution, AMIDS can make use of cryptographic privacy preserving solutions using secure computation and homomorphic encryption techniques that are proposed in the recent AMI security literature. However, deployment of the cryptographic solutions using the existing algorithms would require strong computation capabilities.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VI. CONCLUSION AND FUTURE WORK

In this paper, we presented AMIDS, an integrated intrusion detection solution to identify malicious energy theft attempts in advanced metering infrastructures. AMIDS makes use of different information sources to gather sufficient amount of evidence about an on-going attack before marking an activity as a malicious energy theft. Our experimental results show that through an effective information fusion and using the correlation among the triggered alerts, AMIDS can detect various types of energy theft attempts accurately using individually inaccurate sensors. An autonomous network reconfiguration system (ARS) that enables a multi-radio WMN to autonomously recover from wireless link failures. ARS generates an effective reconfiguration plan that requires only local network configuration changes by exploiting channel, radio, and path diversity. ARS effectively identifies reconfiguration plans that satisfy applications' QoS constraints, admitting up to two times more flows than static assignment, through QoS aware planning. If any failure occur it will automatically reconfigure the node to rectify the problem and each nodes are behave independently and direct communication with the base station. Power scheduling algorithm is used to schedule the usage of power in home area networks, to reduce the usage of electricity. AODV routing protocol is used to control the entire setup of the network. When the power is high, it is mutually supplied to all devices in the network, when it is low; the power is supplied only to the particular devices using priority based scheduling algorithms. Here the future work is hardware implementation of home energy management system to detect energy theft using smart meters.

REFERENCES

[1] C. Bandim, J. Alves Jr, A. Pinto Jr, F. Souza, M. Loureiro, C. Magalhaes, and F. Galvez-Durand(2003) , "Identification of energy theft and tampered meters using a central observer meter: a mathematical approach," in IEEE/PES Transmission and Distribution Conference and Exposition, vol. 1, pp. 163–168.

[2] S. Depuru, L. Wang, V. Devabhaktuni, and P. Nelapati (2011), "A hybrid neural network model and encoding technique for enhanced classification of energy consumption data," in IEEE Power and Energy Society General Meeting, pp. 1–8.

[3] S. Depuru, L. Wang, and V. Devabhaktuni (2010), "A conceptual design using harmonics to reduce pilfering of electricity," in IEEE Power and Energy Society General Meeting, pp. 1–7.

[4] S. Depuru, L. Wang, and V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft (2011)," in IEEE/PES Power Systems Conference and Exposition, pp. 1–8.

[5] S. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi (2010), "Measures and setbacks for controlling electricity theft," in IEEE North American Power Symposium, pp. 1–8.

[6] B. Loeff (2008), "Deputizing data: Using ami for revenue protection," Utility Automation and Engineering.

[7] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. McDaniel (2010),"Multi-vendor penetration testing in the advanced metering infrastructure," in Proc. Annual Computer Security Applications Conference. ACM,pp. 107–116.

[8] McLaughlin, D. Podkuiko, and P. McDaniel (2010), "Energy theft in the advanced metering infrastructure," in Proc. international conference on Critical information infrastructures security. Springer-Verlag, pp. 176–187.

[9] S. McLaughlin, D. Podkuiko, and P. McDaniel (2010), "Energy theft in the advanced metering infrastructure," Critical Information Infrastructures Security, pp. 176–187.

[10] J. Nagi, K. Yap, S. Tiong, S. Ahmed, and A. Mohammad (2008), "Detection of abnormalities and electricity theft using genetic support vector machines," in IEEE TENCON Region 10 Conference, pp. 1–6.

[11] Stephen McLaughlin, Brett Holbert, Ahmed Fawaz, Robin Berthier, and Saman Zonouz (2013), "A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures", Vol 31, no 7.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[12] M. VEILLETTE, "Process for detecting energy theft (2012)," Patent Application US 2012/0 062 210 A1, 03 15. [Online]. Available: http://www.patentlens.net/patentlens/patent/US 2012 0062210 A1/en/.

[13] S. Vukmirovic, A. Erdeljan, F. Kulic, and S. Lukovic (2012), "Software architecture for smart metering systems with virtual power plant," in MELECON 2010-2010 15th IEEE Mediterranean Electrotechnical Conference. IEEE, pp. 448–451.

[14] S. Vukmirovic, A. Erdeljan, F. Kulic, and S. Lukovic (2010), "Software architecture for smart metering systems with virtual power plant," in MELECON 2010-2010 15th IEEE Mediterranean Electrotechnical Conference. IEEE, pp. 448–451.

[15] S. Vukmirovic, A. Erdeljan, F. Kulic, and S. Lukovic, "Software architecture for smart metering systems with virtual power plant," in MELECON 2010-2010 15th IEEE Mediterranean Electrotechnical Conference. IEEE, 2010, pp. 448–451.