IET Cyber-Physical Systems: Theory & Applications

Research Article

Short-term risk assessment of botnet attacks on advanced metering infrastructure

ISSN 2398-3396
Received on 16th March 2017
Revised 7th June 2017
Accepted on 17th July 2017
E-First on 5th September 2017
doi: 10.1049/iet-cps.2017.0047
www.ietdl.org

Kallisthenis I. Sgouras[1] ✉, Avraam N. Kyriakidis[1], Dimitris P. Labridis[1]

[1]*Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 541 24 Thessaloniki, Greece*

✉ *E-mail: ksgouras@ece.auth.gr*

Abstract: An ongoing evolution of the power grids into more intelligent and sophisticated ones has been taking place since the beginning of the 21st century. The underlying objective of the power systems is to deliver electrical energy with high-security standards, i.e. to supply power to the consumers uninterruptedly. However, the integration of information technology into the smart grid introduces new vulnerabilities related to cyber-security which the authors should address extensively. This study discusses the impact of coordinated cyber-attacks on the advanced metering infrastructure. In this work, emulations of distributed denial-of-service attacks in a closed testbed environment using a topology of smart meters that participate in an electricity market are being performed. This study proposes a method to evaluate the impact on the reliability of such attacks. The results demonstrate that the proposed method can serve as a tool for the evaluation of the short-term risk of botnet attacks during load shifting in smart distribution networks.

1 Introduction

1.1 Motivation, objective, and solution

Power supply continuity is a key objective in the reliability studies of the power grids. In recent years, considerable effort has been spent such as GredEx III security exercise [1] to study the power grids' response and recovery from cyber-physical attacks. Smart grid appears to be the next generation of power grids, providing energy with high-reliability standards, while reducing gas emissions and focusing on renewable energy resources and distributed generation. Consequently, smart grid can increase the overall efficiency and sustainability of the power system. In addition, the ability of intentional islanding due to the decentralised production of energy can provide a more robust system [2, 3].

In general, the smart grid can be described as a broadly dispersed network of various interconnected devices that function uninterruptedly to provide a higher degree of reliability and security. Gungor *et al.* in [4] consider the smart grid as a large data communication network, mainly due to the critical role of its communication infrastructure. The wide range of sophisticated devices deployed in smart grids, enables real-time monitoring by the utilities, using measurements collected from sensors placed throughout the grid, and thus providing locational awareness in case of emergency. In this way, the grid becomes self-healing as it can detect and mitigate timely and effectively security failures, a critical feature which is absent in the conventional power grids.

Apart from locational awareness, consumers have the opportunity to participate actively in the electricity market either by controlling the amount of energy they consume or by selling part of their produced energy back to the grid. The utilities can broadcast either price signals to participants in incentive-based demand response (DR) programmes or direct load control commands in emergency cases to reduce the overload probability. These DR actions result in a flattened demand curve which consequently reduces the need for high installed power for peak power plants. Thus, the overall cost-effectiveness of the smart grid is improved [5].

In this work, we consider that the impact of a cyber-attack on the distribution infrastructures is related to the structure of the distribution network and the penetration of controllable power loads. Therefore, we propose a method to assess the short-term risk of a distributed denial-of-service (DDoS) attack on the advanced metering infrastructure (AMI) which handles the electric vehicles (EVs) controllable charging as well as the DR mechanism.

1.2 Literature review

The shift toward a grid with distributed intelligence comes along with critical security issues. Interoperability and heterogeneity are the main features of the smart grid as it will consist of devices and networks of various complexity and diversity. Moreover, incompatibilities between devices might occur [6] as well as proprietary technologies might conceal potential dangers [7]. As a result, security breaches will arise in the less protected areas, introducing new vulnerabilities.

On the other hand, the use of public communication channels is a challenge which might be exploited by malicious users to launch cyber-attacks which will affect the normal grid operation. The motivation can vary from a simple prank to terrorist action, due to the critical nature of the power grid [5]. For example, disgruntled employees could inflict severe damage by attacking critical grid nodes. In other examples of malicious activity, unauthorised access to personal data stored in smart meters might endanger the protection of privacy, and the use of botnets could hinder the actual grid status. Therefore, security measures are fundamental requirements to protect the smart grid operation from the above threats [8]. The American Recovery and Reinvestment Act of 2009 is an example of the effort spent toward the evolution of power grids while also addressing cyber-security threats [2, 9, 10].

The cyber-security problems and the following effects on the power grid are not a new subject of interest in the research community. Manasseh *et al.* in [11] highlight the importance of the communication network between utilities and consumers hosting electrical vehicles. Moreover, researchers in [12] utilised the communication network to activate electrical storage when power fluctuations occurred. Consequently, attackers could consider this particular network as a potential target.

Kang *et al.* in [13] highlight the ability of a man-in-the-middle attack to alter the power flow of a photovoltaic inverter by sending falsified packets, when the attackers have access to the local area network (LAN). Although the above work focuses on the effect on the physical system with a hijacked connection, it does not consider the impact of the loss of availability. On the contrary, the work in [14] approaches the loss of availability problem by simulating DDoS attacks in a topology of smart meters, routers,

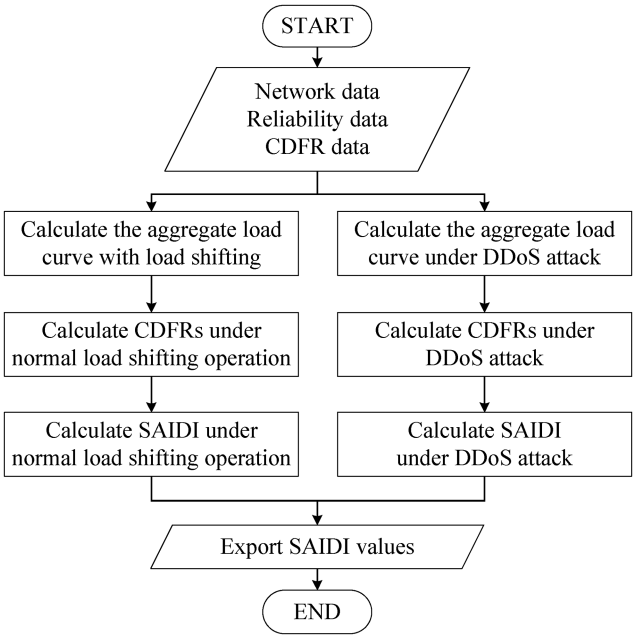

Fig. 1 *Flowchart of the proposed method*

and a utility server. Nevertheless, it does not study the impact on the load curve. Asri and Pranggono in [15] demonstrate the effect on the physical system where they simulate a botnet DDoS attack on a topology of smart meters which are supplied by a wind generator. This paper illustrates the effect of a user datagram protocol (UDP) DDoS attack on the communication channel as well as the loss of power supply during the attack scenario. Although the successful scenario, UDP DDoS attacks can be easily detected and blocked by a firewall. On the other hand, transmission control protocol (TCP) is based on the three-way handshake. As a result, detection mechanisms may not identify the malicious traffic and thus forward it as legitimate, especially when the botmaster spoofs the internet protocol (IP) addresses.

Regarding the advances in the DR technologies and programmes, Paterakis *et al.* in [16] constructed a reference point reviewing DR efforts throughout the world. They provide the *status quo* regarding real-life applications including EV and heating ventilation air-conditioning (HVAC) ones. In [17], a hierarchical DR for EVs via charging stations is studied and a distributed deadline-aware two-level market mechanism is proposed. In [18], a DR control strategy for HVAC is proposed that uses real-time occupancy monitoring with occupancy prediction to achieve efficient conditioning.

In this paper, we evaluate the short-term risk of DDoS attack in a topology of household consumers due to the apparent loss of communication with the server of the DR provider. We take into account the condition-depended failure rates (CDFRs) of the distribution transformer and the main feeder, to calculate their impact on a distribution reliability index, namely the system average interruption duration index (SAIDI). The short-term risk of the DDoS attack is expected to occur by an increased value of SAIDI due to the uncontrolled operation of the controllable loads.

1.3 Contribution

In this paper, we consider that the botmaster has access to the smart grid network. The implemented topology consists of a number of smart meters. Every smart meter represents a household, while the server represents the central point of the topology. The contribution of this work is two-fold. First, we demonstrate as a proof-of-concept, the loss of communication between the server and the consumers due to the DDoS attack. Second, we propose a method for the assessment of the short-term risk of a DDoS attack. The method formulates both the communication network and the power distribution network which hosts controllable power loads. Consequently, the method's algorithm calculates the aggregate power curves during normal and attack scenarios and takes into account CDFRs which in turn may affect the SAIDI values. Finally, the outcome of the proposed method is the tailor-made quantification of the short-term risk of the DDoS attack in the distribution network, expressed as the difference in the SAIDI.

1.4 Paper organisation

The remainder of this paper is organised as follows: Section 2 describes the theoretical background of the modules of the proposed method. More specifically, it describes the architecture of the AMI and DR, followed by important cyber-security issues. Subsequently, it focuses on the most significant cyber-security details and it analyses and formulates DDoS attacks. Section 3 presents the simulation results of the case studies (CSs), and finally Section 4 concludes this paper.

2 Formulation

The proposed method formulates both the communication network and the power distribution network which hosts controllable power loads. As it is shown in Fig. 1, the algorithm collects at the beginning all the input data, i.e. the network, reliability, and CDFR data. Consequently, the algorithm splits into two similar subroutines to calculate in parallel two SAIDI values. One for the normal load shifting operation and one for the DDoS attack scenario. Each subroutine calculates first the aggregate load curve, to determine the CDFRs of the components based on their loading condition, which in turn are needed for the SAIDI calculation. In the last step of the algorithm, the SAIDI values are presented.

2.1 Advanced MI

A fundamental smart grid enabling technology is the AMI, which usually refers to the system that collects measurements and processes various energy usage data from devices throughout the network [19]. AMI allows the system operators to monitor the grid in real time to avoid potential failures and power outages and eventually increase the overall reliability of the grid [14]. For the grid stability, various communication requirements in the different AMI layers provide interoperability and uninterrupted operation in every part of the AMI.

Two-way communication is an essential feature of the AMI, omitted in its ancestor, the advanced meter reading system [4, 20]. To achieve two-way communication between consumers and system operators, the AMI must efficiently provide interconnection between the intelligent devices deployed in every part of the grid, from intelligent electronic devices (IEDs) in substations to smart

meters at the consumers' premises. Thus, electricity and communication data will flow through the network without hindering the normal operation of the grid [21]. Various nodes in the implemented architecture of the AMI perform as such, which is followed in the rest of this paper, and can be divided into three distinctive parts, in accordance with the U.S. Department of Energy [9]:

i. A meter data management system (MDMS) connected via a head end to the rest of the AMI. It is responsible for storing and managing the smart meter's data [21] which are mostly power consumption and communication data exchanged between utilities and consumers [22]. To transmit a large amount of data it uses high-bandwidth technologies such as worldwide interoperability for microwave access (WiMAX), fibre optics or the public Internet. The MDMS is considered an important component of the smart grid.
ii. An aggregation point, otherwise regarded as an interconnected node between the MDMS and the end-use consumers, is employed with the task to implement bidirectional communication between the entities above. It can be considered as a data concentrator from groups of smart meters covering a neighbourhood area network (NAN) to store and forward the necessary data to utilities for further processing. The use in a substation level must allow interoperability between regional and consumer networks that need to communicate effectively to avoid security failures [6].
iii. Smart meters are the local household recorders of electricity consumption, demand, time of use (TOU), and operational data [9]. Implemented as a gateway to the home area network with low-bandwidth requirements, they are entitled to collect forward the above data at specific time intervals [5]. DR signals received by the smart meters influence the real-time household consumption when it is necessary.

The proposed method is applied to the distribution level of the network which spans from the distribution transformer to the consumers' appliances. Therefore, it is expected that the topologies under study will host a number of 100–500 consumers. Various household devices are considered to be installed in each house such as refrigerators, washing machines, lighting devices, and HVAC system. It is also assumed that an EV charger is connected in a pre-defined number of households.

2.2 Demand response

Among the smart meter capabilities, the remote load influence can be considered the most pioneering one, as it allows consumers to participate actively in the electricity market. DR signals can be either mandatory or voluntary requests for load curtailment in the form of a price signal. Consumers may choose to accept the price incentives to maximise their profit. For the utility company, real-time pricing (RTP) signals can result in significant peak-shaving, especially in high-demand periods, reducing the risk of failure and eventually increasing the reliability of the grid.

In the current approach, we divide the consumers into active and unresponsive ones. The members of the first group participate actively in an RTP market by following the price signals from a central server, while the others use their appliances when needed, regardless the price signal. The response to price signals is automatic without human interference. Participants send their bids to an electricity market which collects and sorts the bids and transmits back the appropriate price signal. The price after the electricity market closes determines in which households a switch-off command of the controlled devices will be performed. In this paper, the EV charging and the HVAC systems are considered as the only controllable power loads by the electricity market. In the EV charging case, the load can be shifted in off-peak periods to reduce the overall power consumption during peak hours. Accordingly, in the HVAC case, a responsive consumer may accept a switch-off during peak hours.

2.3 Cyber-security

Information technology and computer networks are widely embedded and are supposed to increase rapidly the complexity of the smart grid [5, 21]. Combining this factor with the large-scale nature of the grid, security in every part of this newly introduced grid will be an impossible task [23]. Moreover, the interconnection of networks and systems of different technical characteristics, from generation to consumption, which will hardly be owned by the same entity, introduces various new vulnerabilities [24].

Cyber-security has been addressed as a priority for the broad implementation of the smart grid, according to Locke and Gallagher [25], and is a major impediment to the ongoing development of the smart grid. European countries such as Germany have delayed the installation of smart meters due to privacy issues [9]. Therefore, security requirements must be fulfilled to address the problem effectively.

Considering the smart grid as a network of bidirectional exchange of information, the basic information security requirements are confidentiality, integrity, and availability. Alternatively, these definitions can be substituted by interception, modification, and interruption, respectively, as stated in [24]. Reference [3] considers the availability as the prime requirement for the reliable management of the power grid. Consequently, the rest of this paper focuses on the loss of availability of the transmitted information and its outcome on the underlying power grid.

2.4 DDoS attacks

The main contribution of this paper is to demonstrate the impact of a DDoS attack and consequently the loss of availability in the smart grid. Unlike a DoS attack where the attacker makes the target unavailable to its legitimate users, a DDoS attack is a coordinated DoS attack where the attacker exploits multiple compromised systems such as botnets, to cause greater damage to the target. More specifically, a DDoS attack can deplete the computational resources of the target and cause serious delay or even failure in the data transmission through the communications channel [5, 6, 26]. Such attacks might have severe consequences regarding critical infrastructures. For example, a delay of some milliseconds in a mandatory load disconnection command can result in a significantly increased load during a period when its curtailment would be crucial to avoid overload of the grid.

We examine the use of botnets to initiate highly coordinated DDoS attacks considering that the topology uses public communication channels in parts of the smart grid network. Public Internet access will serve as the necessary entry point for the botmaster to gain access to the internal network and initiate a coordinated attack. According to [27], public Internet is considered as a possible communication path between utility providers and consumers. More specifically, it states that the Internet can be used in the communication between third-party services, which in this work is considered the main server, and the consumers. Therefore, DR messages, load control, and remotely switch-off commands are dispatched through the Internet, making its adoption as a communications path a realistic case scenario.

A DDoS attack can transcend from the communication channels to the physical system of the power distribution. Cyber-physical security [5, 28] is a growing issue in the field of smart grid cyber-security. A characteristic example of cyber-physical security threat is when a switch-off command is sent to an IED that controls a circuit breaker remotely, and due to a DDoS attack, the command fails to reach its destination resulting in possible equipment failure or even power outage [13]. GridEx II [29] demonstrates the importance of cyber-physical security in the exercise of the North American Electric Reliability Corporation, where the ability of the power grid to deal with the adverse situations of a cyber-attack is examined thoroughly.

Regarding the communication technologies in AMIs, WiMAX can be considered secure and reliable, offering a wide coverage of 50 km and data rates of 70 Mbps, suitable for DR applications. Additionally, authentication mechanisms are an inherent part of WiMAX as encryption techniques, and standards make packet

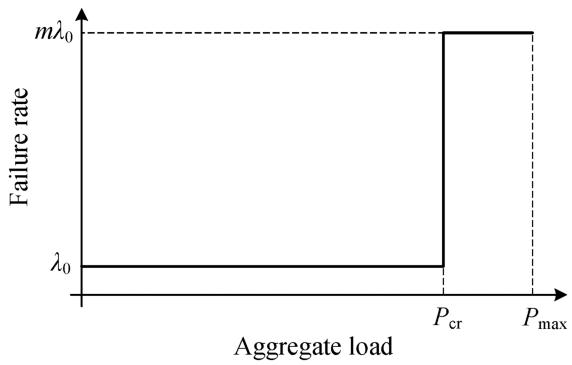

Fig. 2 *Condition-dependent failure rate model. For light loading conditions the failure rate is λ_0. For higher loading, the failure rate is multiplied by a factor m*

sniffing difficult. Consequently, sensitivity to compromise is low in this case; however, it is still possible to perform a successful DDoS attack to the system effectively [30]. The utilisation of cellular technologies is an alternative solution to WiMAX, and they are advantageous due to the wide coverage even in remote places. General packet radio service (GPRS) offers strong security protocols for data transmission as well as a range of authentication mechanisms that make the packet sniffing procedure a demanding task. However, Traynor *et al.* in [31] demonstrated that a botnet of poorly secured mobile phones could be utilised to cause significant availability issues in the examined cellular network. The present work aims to address the increasingly sophisticated attacks that may occur in such networks. Therefore, as GPRS utilises IP-based protocols, the examined DDoS attack can be a potential threat. In addition, low data rate, low quality-of-service during peak hours, and availability issues in critical conditions, as stated in [32], could ensure the communication congestion in GPRS in the case of a DDoS attack. For these reasons, in this paper, we focus on WiMAX technologies for the communication between data concentrators and servers.

Regarding the potential number and type of the devices that could initiate a coordinated attack, there are reports in current bibliography such as the Mirai case [33] that raise the number too many thousands of Internet-connected devices such as closed-circuit televisions and IP cameras, printers, and wireless routers. Mirai software was used to launch the large-scale 2016 Dyn cyber-attack that resulted in major Internet platforms be unavailable for a period. The same report states that more than 145,000 compromised IoT devices that formed part of a botnet were utilised for the attack that occurred in OVH web-hosting provider. The cost of launching such attacks can be varied per several parameters, e.g. the target characteristics, the source of the attack, and the attack scenario. A recent report [34] collects some current tariffs for the hire of DDoS resources. For example, a 3 h DDoS attack would cost $60.

In this work, we focus on TCP Synchronise (SYN) sequence number flood DDoS attacks using a botnet. The conducted experiments aim to address the serious issue of initiating a DDoS attack when part of the communications infrastructure lies on the public Internet, and therefore its vulnerabilities are inherited in the smart grid. We assumed that only the communication between the aggregation point and the main server is deployed via the Internet, whereas the rest of the communication between the aggregation point and the meters utilise IP-based protocols. As a result, the botmaster can gain access to the smart grid communication network while utilising techniques such as packet sniffing, so that the IP address of the central server can be acquired to launch an attack. The attacks target the server because attacking a single smart meter has insignificant interest [21, 35].

2.5 CDFR and SAIDI

To analyse the impact of a DDoS attack on the physical system especially on peak hours, we use the CDFR of the main distribution components during the attack. These components are the power transformer, and the main power distribution line, also known as main feeder. According to [36–40] the failure rate of the power distribution components should be considered as a function of loading. Since there is not any standard method for the modelling of the CDFR of a component, we use the CDFR model as shown in Fig. 2. It is expected that potential network overload due to uncontrolled operation of the controllable power loads will have a negative effect on the distribution reliability. In addition, lower reliability means higher risk [41].

In this work, excluding the power transformer and the main feeder, we assume that all the other distribution components, as well as the upstream transmission system, are fully reliable. We calculate the availability A of the transformer and the main feeder, using the mean time between failures, mean time to repair (MTTR), and mean failure rate as follows:

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \tag{1}$$

where MTBF = 1/MFR.

Owing to the series connection of the transformer and the main feeder, the expected system unavailability U_S, is

$$U_{\text{S}} = 1 - A_{\text{T}} \cdot A_{\text{F}} \tag{2}$$

where A_{T} and A_{F} are the availability of the transformer and the main feeder, respectively.

The U_{S} can be expressed in an annual term, as the system unavailability over the course of a year, to represent the expected interruption duration which every consumer sustains during a year. By definition, this metric equals to the SAIDI. To sum up, the network components that are characterised by CDFR, trigger spontaneous interruptions, which in turn are logged by SAIDI values regarding the annual average interruption duration for each consumer. Finally, the attack impact on the SAIDI value is assumed as the short-term risk of cyber-attack in terms of increased consumer interruption probability.

3 CSs and discussion

This section presents the simulation results of four CSs, namely CS1–CS4, to estimate the impact of a DDoS attack on the smart grid infrastructure in both the communications network and the power infrastructure. The simulations are grouped into two distinctive sections. First, we emulate a massive DDoS attack, applied by a botnet on a closed testbed environment (CS1–CS2), and second we integrate the drawn results to a smart grid topology of 300 smart meters with 150 EVs (CS3–CS4) to present the impact on the power grid. We use the CS1 and CS2 as a proof-of-concept, while in the CS3 and CS4 we calculate the DDoS impact.

3.1 DDoS attack on the central server

For the DDoS attack in CS1 and CS2, we use the Botnet Simulator (BoNeSi) [42] which employs a botnet of 50,000 bots to perform a DDoS attack. BoNeSi can generate realistic traffic patterns such as TCP and UDP data flows to simulate a DDoS attack successfully.

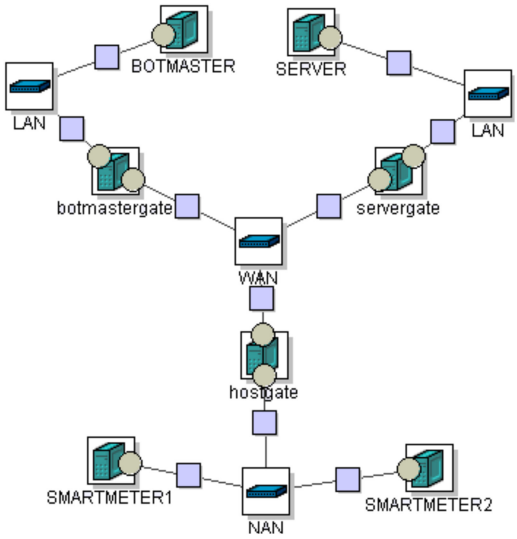

Fig. 3 *Emulated topology in Emulab*

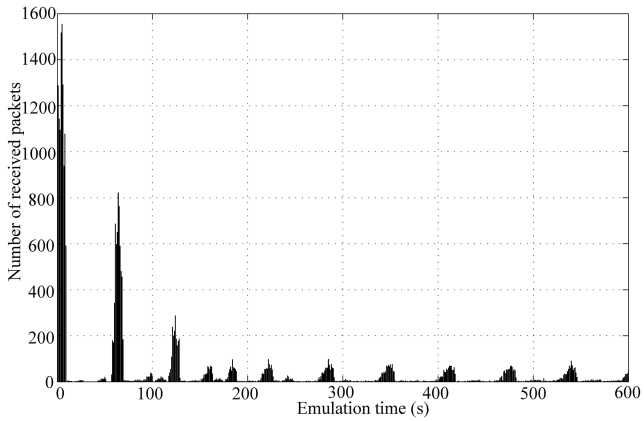

Fig. 4 *CS1 – Botnet DDoS attack on the server*

Moreover, the simulator allows the specification of various parameters such as data volume, the number of IP addresses, and the total packets per second that are being sent to the targets. Regarding the TCP/SYN flood DDoS attack, BoNeSi must be combined with a closed testbed environment. For this purpose, we use the Emulab testbed [43, 44], because the TCP answers from the server must be routed back to the BoNeSi to extract the results.

Fig. 3 shows the emulated topology. It consists of a web server, the target of the attack, which can be deemed as the central server of the AMI, broadcasting data and price signals to smart meters. Two smart meters and the BoNeSi machine are running; otherwise, known as the botmaster which is the attacking node. Hostgate also can be considered as a data concentrator for the group of smart meters, to implement bidirectional communication between the group and the main server. Since it is impractical to use more than 300 real machines in the testbed to emulate the smart meters and allocate IP addresses, we present selected key features of the proposed topology. Albeit, the smart meters are not participating actively in the attack scenario, they attempt to communicate with the server to evaluate whether the server can communicate with the healthy devices during the attack.

In this work, the graphic user interface of Emulab is used to design the specified topology. The wireless area network (WAN) where both the server and the botmaster are connected is assumed to be the public Internet. We implement the dedicated connections between the two entities and the LANs by broadband network infrastructures such as fibre optics or WiMAX due to the large traffic volume that flows in these sub-networks. On the other hand, we use low-bandwidth technologies such as ZigBee in the smart meter connections. We present in the Appendix the specific bandwidth connection details, as well as web traffic characteristics that we use in the BoNeSi emulation.

Table 1 CS2 –web server ping attempt under botnet DDoS attack

Moment of ping transmission, s	Duration until rejection, s	Outcome
60	480.80	rejected
570	382.41	rejected
960	526.62	rejected
1500	368.75	rejected
1890	414.22	rejected
2310	745.95	rejected
3060	365.45	rejected
3450	166.49	aborted – end of simulation

In CS1, we initiate a DDoS attack by the botmaster toward a server, utilising every bot available in the botnet. When the simulation begins, the bots flood the server with TCP packets. The attacker targets the communication infrastructure of the smart grid once he manages to gain access through the public Internet. In Fig. 4, the total number of TCP packets per second that are successfully received by the botmaster are shown when the target is the server of the topology in a real-time 10 min emulation. The packets represent the answers from the server to the initial TCP requests that are sent by the bots. The gradual decrease in the number of received packets depicts the incompetence of the server to respond to incoming traffic.

Apart from the packet received rate, we examine the ability of the smart meter to communicate with the server and send metering data during the attack scenario. For that case, we model a typical computer in the Emulab topology to represent the smart meter of a household which participates in the electricity market.

As we consider that an hourly isolation of a smart meter could have a non-negligible influence on the aggregate power load, we implement a 60 min CS, the CS2, where the SMARTMETER1 from the above topology sends a TCP request to the web server to test its availability. The ping sequence is set to start by the 60th second of the emulation, with a maximum of 20 retry attempts. Table 1 lists the results of this emulation, where we observe only rejection messages.

CS1 and CS2 demonstrate the gradual unavailability of the topology server and the incompetence of the household smart meter to send consumption measurements to extract price signals for the RTP market that the HVAC participates and the TOU market that the EV participates. CS1 demonstrates that the constant requests being sent from the bots eventually floods the communication channel of the server resulting in an inability of communicating with the meters. Similarly, CS2 shows the meters' efforts to send its measurements to the central server during the 1 h scenario that is examined. Each meter starts sending a packet after the first minute of the emulation. When the packet is aborted, it is being resent automatically until 20 efforts are reached the packet is finally rejected. Subsequently, a new packet is sent and the procedure continues until the end of emulation.

3.2 DDoS impact on the power distribution network

In the second part of the simulations (CS3–CS4) we use GridLAB-D [45], where we deploy the topology of the distribution network for 300 households. GridLAB-D is a power distribution simulation tool which gives valuable insight into the operation of the distribution network while integrating new technologies such as EVs. When combined with the framework for network co-simulation (FNCS), it allows the users to model both the communications network and the power infrastructure of a smart grid. More specifically, GridLAB-D models the power network, whereas network simulator 3 (ns-3) [46] is employed to construct the communications topology. Subsequently, FNCS ensures the cooperation of these different simulation environments especially in cases where multiple households participate in electricity markets with the dispatch of price signals.

In the simulation environment, we assume that a group of the households participates in the electricity market that controls the usage of the HVAC cooling system. We also assume that a DDoS attack occurs during the summer days when cooling demand is increased. The bid price and quantity are determined based on the current indication of the thermostat of each house and the comfort zone that each consumer specifies in collaboration with the utility company. The comfort zone is defined as the upper limit that each consumer allows the temperature to climb before the house becomes too hot. For example, unspecified comfort zone indicates zero participation in the electricity market for this consumer who is considered as unresponsive one and his electricity demand is considered inelastic. On the basis of the current air temperature, consumers send their bids, which are forwarding through ns-3 via communication channels of specified bandwidth, to the market which collects and sorts them. Afterwards, the market broadcasts its clearing price to the participants, and the appliances are switched on in the case of bid acceptance. Otherwise, the consumer can bid again in the next market timeslot which occurs every 5 min. Although the load control is restricted in the HVAC, the results can be expanded in cases where multiple EDs participate in the market.

Apart from the HVAC system, we implement a second market which controls the charging of the EVs. We model two types of EVs, and their characteristics can be found in the Appendix. The market for the EVs is based on a TOU programme. More specifically, during the day, a high price signal is broadcast to the households to prevent the vehicles from charging during the peak hours of the day. During the night, when the demand is relatively low, the charging is promoted, and the market allocates the EV charging load in such a way to avoid unexpected peaks in the load curve. Through this procedure, we manage to model the load shifting from peak hours to off-peak hours, during the night. We examine a 50% EV penetration, i.e. 150 households host an EV (50× Type 1 and 100× Type 2). We use the reliability data for the transformer and the main feeder from [47], as listed in Table 2. The simulation results are presented in the following paragraphs.

3.2.1 SC3 –market participation: Fig. 5 illustrates the importance of participating in an RTP market which can shift part of the load to off-peak hours. In this scenario, we assume that EV charging is an elastic load that can be shifted to the night when the market price is low. Furthermore, the load distribution should be as smooth as possible to avoid unexpected peaks.

3.2.2 SC4 – DDoS attack impact on the grid: To incorporate the obtained results from CS1 and CS2, we assume that each participating household in the RTP market behaves as if it was unresponsive in the beginning. In other words, there is no tolerance in the temperature rise or fall in the house, and the HVAC is utilised whenever the temperature changes above or below a pre-specified value. Consequently, as the main server does not receive any bid from the participating customers as a result of the DDoS attack, it considers them as unresponsive, and therefore must meet their demand for power in each moment. Regarding the EV charging, the modelled chargers take as input the arrival time of each car depending on various implemented scenarios. It should be mentioned that the EVs do not charge during their absence from the household and their day trip is pre-defined. The participation of the EVs in the TOU market starts from 11 pm until 7 am on the next day. During that time, the procedure takes into account the initial demand at the beginning of the TOU market and calculates the difference between this value and the power consumption in the case where no cars are charging during the night (red curve in Fig. 5) for 5 min intervals. Gradually, the system allows more cars to charge, by considering the full EV capacity and the requirement that each car must be fully charged before leaving the house, to fill smoothly the valley in the power consumption during the night without imposing new peaks. When a DDoS attack occurs, it is assumed that there is no communication between the server and the charger, and therefore the EVs charge as they arrive at home as none price incentive is imposed during that time to shift their load to off-peak hours. As a result, an uncontrolled EV charging happens during the DDoS attack scenario.

Table 2 CDFR data

Network element	P_{cr}/P_{max}	λ_0	MTTR, h	m
power transformer	0.9	0.015/year	200	15
main feeder	0.9	0.065/year	5	10

Fig. 6 depicts the 24 h aggregate power consumption comparison between the regular DR operation, where we apply load shifting and the respective attack situation of total communication loss in the communications network due to the DDoS attack. We can observe that between 12 am to 8 am the valley filling of the aggregate load curve cannot be achieved because the DDoS attack prevents the scheduled operation of the controllable loads. As a result, the HVAC systems and the EV charging are served uncontrollably during the day.

Apart from the overall impact of the DDoS attack in the shape of the demand curve, Figs. 7 and 8 depict the period of time during the transformer and the main feeder are stressed with load ≤90% of the initial peak load. We can observe that during the attack, the load is constantly >90% of the initial peak for 265 min (4.417 h), compared with the base case where the peak load occurs sporadically for a total time of 10 min (0.167 h).

In the final step, we use the reliability and the CDFR data, as they are stated in Table 2, to calculate the impact of the DDoS attack on the SAIDI by (1) and (2). The simulation and calculation results are listed in Table 3.

The short-term risk of a DDoS attack on a distribution network is quantified in terms of SAIDI value by the proposed method. We calculate that during a DDoS attack, the consumers can be exposed to a nearly double system unavailability and SAIDI value. In other

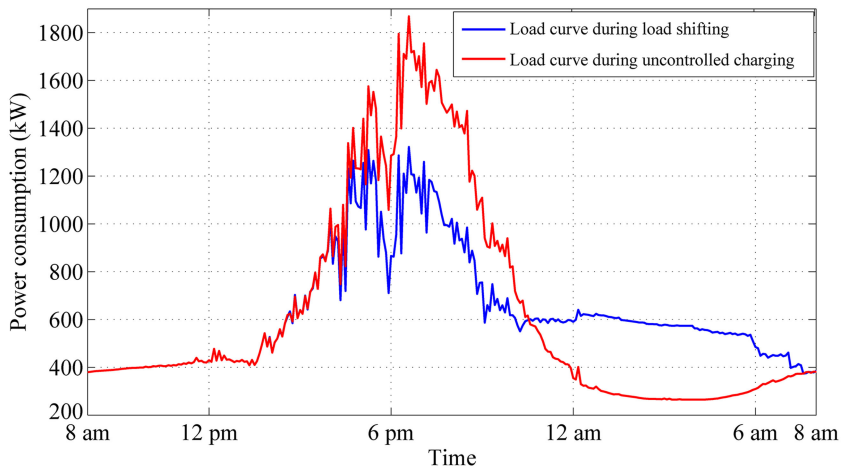

Fig. 5 *CS3 – load control with 50% EV penetration*

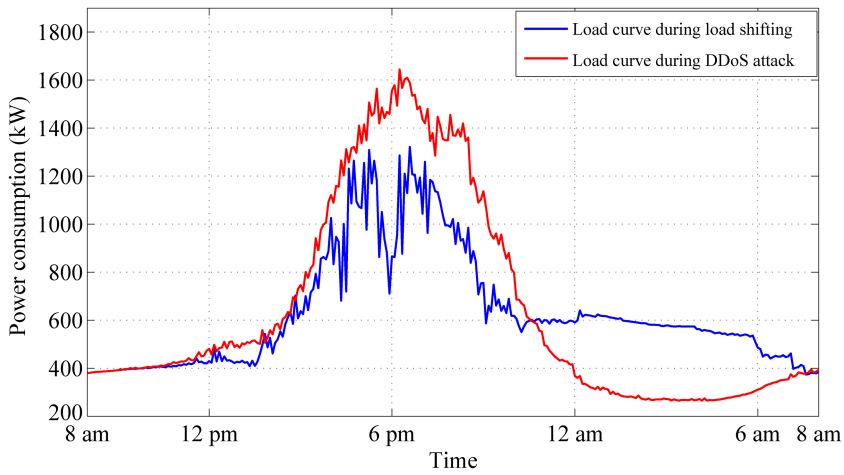

Fig. 6 *CS4 – loss of communication due to DDoS attack*

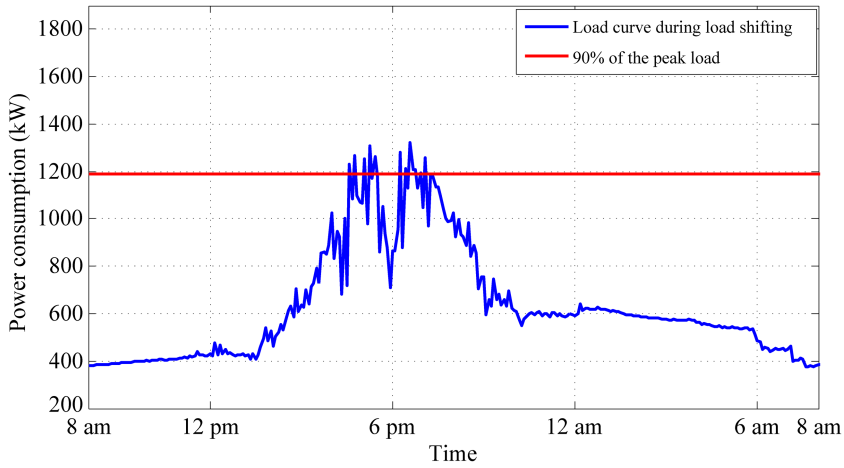

Fig. 7 *Excessive load >90% with load control*

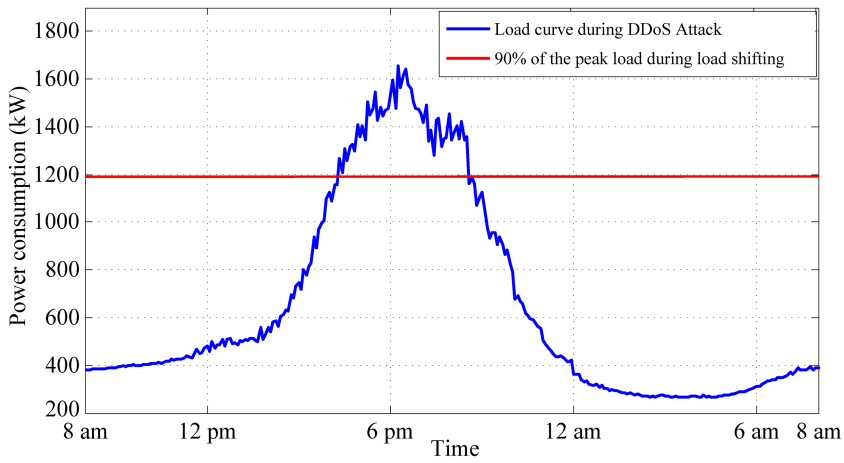

Fig. 8 *Excessive load in DDoS attack*

Table 3 Results of CS3 and CS4

CS	Peak period	U_S	SAIDI, h/year
CS3	0.167 h	0.0003937	3.45
CS4	4.417 h	0.0007565	6.63

words, such attacks may multiply the short-term expected interruption probability, as it is shown in the above CSs.

A modern distribution network operator (DNOs) might operate under performance-based regulation regarding the SAIDI value. Currently, in Europe, various reward and penalty schemes have been applied in 17 countries [48]. In such cases, the annual SAIDI performance could result in rewards or penalties imposed by the regulation targets. Therefore, the proposed method could be useful to calculate the impact of controllable loads in the reliability performance. Concluding, a DNO could use the proposed method to estimate specific risk management actions, e.g. penetration limits of controllable loads, to avoid the risk of performance penalties due to DDoS attacks.

4 Conclusion

This paper investigates the ability of botnets to infiltrate the communication network of the smart grid and initiate a DDoS attack and it proposes a method for the short-term risk assessment. The method evaluates the risk in terms of the impact on the SAIDI

value of distribution network, taking into account controllable loads as EVs and HVAC.

We used the BoNeSi for the DDoS attacks, and the graphical user interface of Emulab to design the topology for the proof-of-concept. To calculate the short-term risk, we modelled the distribution network and its communication infrastructure with the collaboration of GridLAB-D, FNCS, and ns-3.

Finally, CSs have been presented to demonstrate the capability of the proposed method. The method can be used by a DNO as a decision support system for the calculation of the maximum penetration of controllable loads, according to the desired risk tolerance.

5 Acknowledgments

This work was supported by the State Scholarships Foundation of Greece in the context of the "IKY Fellowships of Excellence for Postgraduate studies in Greece - Siemens Program".

6 References

[1] NERC: '*Grid security exercise 2015 (GridEx III) public report*' (NERC, 2015), pp. 1–23

[2] Hamilton, B.A., Miller, J., Renz, B.: '*Understanding the benefits of the smart grid – smart grid implementation strategy*' (National Energy Technology Laboratory, DoE, USA, 2010), pp. 1–41

[3] Smart Grid Interoperability Panel Cyber Security Working Group: '*Introduction to NISTIR 7628 guidelines for smart grid cyber security*' (NIST, USA, 2014), pp. 1–597

[4] Gungor, V.C., Sahin, D., Kocak, T., *et al.*: 'A survey on smart grid potential applications and communication requirements', *IEEE Trans. Ind. Inform.*, 2013, **9**, (1), pp. 28–42, doi: 10.1109/TII.2012.2218253

[5] Mo, Y., Kim, T.H.J., Brancik, K., *et al.*: 'Cyber-physical security of a smart grid infrastructure', *Proc. IEEE*, 2012, **100**, (1), pp. 195–209, doi: 10.1109/JPROC.2011.2161428

[6] Li, X., Liang, X., Lu, R., *et al.*: 'Securing smart grid: cyber attacks, countermeasures, and challenges', *IEEE Commun. Mag.*, 2012, **50**, (8), pp. 38–45, doi: 10.1109/MCOM.2012.6257525

[7] Janicke, H., Nicholson, A., Webber, S., *et al.*: 'Runtime-monitoring for industrial control systems', *Electronics*, 2015, **4**, (4), pp. 995–1017, doi: 10.3390/electronics4040995

[8] Eder-Neuhauser, P., Zseby, T., Fabini, J.: 'Resilience and security: a qualitative survey of urban smart grid architectures', *IEEE Access*, 2016, **4**, pp. 839–848, doi: 10.1109/ACCESS.2016.2531279

[9] Bhat, K., Sundarraj, V., Sinha, S., *et al.*: '*IEEE cyber security for the smart grid*' (IEEE, 2013), pp. 1–122, doi: 10.1109/IEEESTD.2013.6613505

[10] 'American recovery and reinvestment act of 2009', an act of the congress of the United States of America Publ. L. No. 111-5, February 2009

[11] Manasseh, E.C., Ohno, S., Yamamoto, T., *et al.*: 'Distributed demand-side management optimisation for multi-residential users with energy production and storage strategies', *J. Eng.*, 2014, pp. 1–8, doi: 10.1049/joe.2014.0199

[12] Godfrey, T., Mullen, S., Griffith, D.W., *et al.*: 'Modeling smart grid applications with co-simulation'. Proc. First IEEE Int. Conf. Smart Grid Communications, Gaithersburg, MD, USA, October 2010, pp. 291–296, doi: 10.1109/SMARTGRID.2010.5622057

[13] Kang, B., Maynard, P., McLaughlin, K., *et al.*: 'Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations'. Proc. 20th Conf. Emerging Technologies Factory Automation, Luxembourg City, Luxembourg, September 2015, pp. 1–8, doi: 10.1109/ETFA.2015.7301457

[14] Sgouras, K.I., Birda, A.D., Labridis, D.P.: 'Cyber attack impact on critical smart grid infrastructures'. Proc. IEEE PES Innovative Smart Grid Technologies Conf. (ISGT 2014), Washington, DC, USA, February 2014, pp. 1–5, doi: 10.1109/ISGT.2014.6816504

[15] Asri, S., Pranggono, B.: 'Impact of distributed denial-of-service attack on advanced metering infrastructure', *Wirel. Pers. Commun.*, 2015, **83**, (3), pp. 2211–2223, doi: 10.1007/s11277-015-2510-3

[16] Paterakis, N.G., Erdinç, O., Catalão, J.P.S.: 'An overview of demand response: key-elements and international experience', *Renew. Sustain. Energy Rev.*, 2017, **69**, pp. 871–891, doi: 10.1016/j.rser.2016.11.167

[17] Fanxin, K., Xue, L.: 'Distributed deadline and renewable aware electric vehicle demand response in the smart grid'. Real-Time Systems Symp., Washington, DC, USA, December 2015, pp. 23–32, doi: 10.1109/RTSS.2015.10

[18] Erickson, V.L., Cerpa, A.E.: 'Occupancy based demand response HVAC control strategy'. Proc. Second ACM Workshop Embedded Sensing Systems for Energy-Efficiency in Building, Zurich, Switzerland, November 2010, pp. 7–12, doi: 10.1145/1878431.1878434

[19] Yan, Y., Qian, Y., Sharif, H.: 'A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid'. Proc. Wireless Communications Networking Conf., Cancún, Mexico, March 2011, pp. 909–914, doi: 10.1109/WCNC.2011.5779257

[20] Fang, X., Misra, S., Xue, G., *et al.*: 'Smart grid – the new and improved power grid: a survey', *IEEE Commun. Surv. Tutor.*, 2011, **14**, (4), pp. 944–980, doi: 10.1109/SURV.2011.101911.00087

[21] Liu, J., Xiao, Y., Li, S., *et al.*: 'Cyber security and privacy issues in smart grids', *IEEE Commun. Surv. Tutor.*, 2012, **14**, (4), pp. 981–997, doi: 10.1109/SURV.2011.122111.00145

[22] Yu, K., Arifuzzaman, M., Wen, Z., *et al.*: 'A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid'. Proc. Int. Conf. Power System Technology (POWERCON 2014), Chengdu, China, October 2014, pp. 2019–2024, doi: 10.1109/TIM.2015.2444238

[23] Wang, W., Lu, Z.: 'Cyber security in the smart grid: survey and challenges', *Comput. Netw.*, 2013, **57**, (5), pp. 1344–1371, doi: 10.1016/j.comnet.2012.12.017

[24] He, D., Chen, C., Bu, J., *et al.*: 'Secure service provision in smart grid communications', *IEEE Commun. Mag.*, 2012, **50**, (8), pp. 53–61, doi: 10.1109/MCOM.2012.6257527

[25] Locke, G., Gallagher, P.D.: '*NIST framework and roadmap for smart grid interoperability standards, Release 1.0*' (NIST, USA, 2010), pp. 1–145

[26] Barroso, D.: '*Botnets – the silent threat*' (ENISA, 2007), pp. 1–12

[27] IEEE Std. 2030–2011: 'IEEE guide for smart grid interoperability of energy technology and information technology operation with the Electric power system (EPS), end-use applications, and loads', 2011, doi: 10.1109/IEEESTD.2011.6018239

[28] Sridhar, S., Hahn, A., Govindarasu, M.: 'Cyber-physical system security for the electric power grid', *Proc. IEEE*, 2012, **100**, (1), pp. 210–224, doi: 10.1109/JPROC.2011.2165269

[29] NERC: '*Grid security exercise (GridEx II) after-action report*' (NERC, 2014), pp. 1–26

[30] Barbeau, M.: 'WiMax/802.16 threat analysis'. Proc. First ACM Int. Workshop on Quality of Service & Security in Wireless and mobile networks'. Montreal, Quebec, Canada, October 2005, pp. 8–15, doi: 10.1145/1089761.1089764

[31] Traynor, P., Lin, M., Ongtang, M., *et al.*: 'On cellular botnets: measuring the impact of malicious devices on a cellular network core'. Proc. 16th ACM Conf. Computer and Communications Security, Chicago, IL, USA, November 2009, pp. 223–234, doi: 10.1145/1653662.1653690

[32] Usman, A., Shami, S.H.: 'Evolution of communication technologies for smart grid applications', *Renew. Sustain. Energy Rev.*, 2013, **19**, pp. 191–199, doi: 10.1016/j.rser.2012.11.002

[33] Enisa: 'Major DDoS attacks involving IoT devices'. Available at https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices

[34] Makrushin, D.: 'The cost of launching a DDoS attack'. Available at https://securelist.com/analysis/publications/77784/the-cost-of-launching-a-ddos-attack

[35] Khurana, H., Hadley, M., Lu, N., *et al.*: 'Smart-grid security issues', *IEEE Secur. Priv.*, 2010, **8**, (1), pp. 81–85, doi: 10.1109/MSP.2010.49

[36] Zhu, D.: 'Electric distribution reliability analysis considering time-varying load, weather conditions and reconfiguration with distributed generation'. PhD thesis, Virginia Polytechnic Institute and State University, 2007

[37] Brown, R.E.: '*Electric power distribution reliability*' (CRC Press, Boca Raton, FL, 2008, 2nd edn.)

[38] Sun, Y., Cheng, L., Liu, H., *et al.*: 'Power system operational reliability evaluation based on real-time operating state'. Proc. Int. Power Engineering Conf., Singapore, November 2005, pp. 722–727, doi: 10.1109/IPEC.2005.207002

[39] Sun, Y., Wang, P., Cheng, L., *et al.*: 'Operational reliability assessment of power systems considering condition-dependent failure rate', *IET Gener. Transm. Distrib.*, 2010, **4**, (1), pp. 60–72, doi: 10.1049/iet-gtd.2009.0006

[40] He, J., Cheng, L., Sun, Y.Z.: 'Transformer real-time reliability model based on operating conditions', *J. Zhejiang Univ. Sci. A*, 2007, **8**, (3), pp. 378–383, doi: 10.1631/jzus.2007.A0378

[41] Li, W.: '*Risk assessment of power systems: models, methods, and applications*' (John Wiley & Sons, Inc., New York, 2014, 2nd edn.)

[42] 'BoNeSi DDoS botnet simulator'. Available at https://github.com/Markus-Go/bonesi

[43] 'Emulab – network emulation testbed'. available at http://www.emulab.net

[44] White, B., Lepreau, J., Stoller, L., *et al.*: 'An integrated experimental environment for distributed systems and networks'. Proc. Fifth Symp. Operating Systems Design Implementation (OSDI '02), Boston, MA, USA, December 2002, pp. 255–270, doi: 10.1145/844128.844152

[45] Chassin, D.P., Schneider, K., Gerkensmeyer, C.: 'GridLAB-D: an open-source power systems modeling and simulation environment'. Proc. IEEE PES T&D Conf. and Exposition, Chicago, IL, USA, April 2008, pp. 1–5, doi: 10.1109/TDC.2008.4517260

[46] Riley, G.F., Henderson, T.R.: 'The ns-3 network simulator', in Wehrle, K., Güneş, M., Gross, J. (EDs.): '*Modeling and tools for network simulation*' (Springer Berlin Heidelberg, 2010), pp. 15–34, doi: 10.1007/978-3-642-12331-3_2

[47] Allan, R.N., Billinton, R., Sjarief, I., *et al.*: 'A reliability test system for educational purposes-basic distribution system data and results', *IEEE Trans. Power Syst.*, 1991, **6**, (2), pp. 813–820, doi: 10.1109/59.76730

[48] CEER: 'Benchmarking report 5.2 on the continuity of electricity supply', February 2015, pp. 1–54

6 Appendix

6.1 Simulation parameters

See Tables 4–6.

Table 4 Topology parameters

SMARTMETER-to-NAN	0.768 Mbps
NAN-to-hostgate	155 Mbps
hostgate-to-WAN	1000 Mbps
BOTMASTER-to-LAN	10 Mbps
LAN-to-botmastergate	155 Mbps
botmastergate-to-WAN	1000 Mbps
SERVER-to-LAN	100 Mbps
LAN-to-servergate	155 Mbps
servergate-to-WAN	1000 Mbps

Table 5 Web traffic

packet payload	32 B
packets per second	5000
destination port	22

Table 6 EV types

	Type 1	Type 2
battery size	70 kWh	17.1 kWh
charging efficiency	0.92	0.9
charge rate	10 kW	3.6 kW
electric range	240 miles	53 miles