Wireless Pers Commun (2015) 83:2211–2223
DOI 10.1007/s11277-015-2510-3

Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure

Satin Asri · Bernardi Pranggono

Published online: 12 March 2015

Abstract The age of Internet of Things has brought in new challenges specifically in areas such as security. The evolution of classic power grids to smart grids is a prime example of how everything is now being connected to the Internet. With the power grid becoming smart, the information and communication systems supporting it is subject to both classical and emerging cyber-attacks. The article investigates the vulnerabilities caused by a distributed denial-of-service (DDoS) attack on the smart grid advanced metering infrastructure. Attack simulations have been conducted on a realistic electrical grid topology. The simulated network consisted of smart meters, power plant and utility server. Finally, the impact of large scale DDoS attacks on the distribution system's reliability is discussed.

Keywords Advanced metering infrastructure (AMI) · Distributed denial-of-service (DDoS) · Smart grid · Smart meter

1 Introduction

In 2011 McAfee reported over 60 % of critical infrastructure companies regularly found malware designed to attack their systems. Smart grid is arguably the most fundamental cyber-physical infrastructures of humankind and modern society. Smart grid and advanced metering infrastructure (AMI) or commonly known as the smart meter are considered as the main signs of classical electrical grid's evolution toward smarter grids. The new grid promises to improve energy efficiency and reliability by incorporating information

S. Asri
Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal, India
e-mail: satinasri@gmail.com

B. Pranggono (✉)
School of Engineering and Built Environment, Glasgow Caledonian University, Glasgow, UK
e-mail: bern@ieee.org; b.pranggono@gcu.ac.uk

communication technologies (ICT), renewable energy generation, new transmission and distribution technologies, increased levels of automation and control, and Internet of Things (IoT) technologies consisting of sensors/actuators, sensor networks, analytics, data, and information.

It is expected that smart meters would be rolled-out worldwide in the next decade. For example, in the US it is expected that 60 million smart meters would be installed by 2015 and the UK government has plans to roll-out smart meters in every home by 2020. By replacing classical electric meters with smart meters, a wide range of functionalities can be provided to the customers, energy providers and third parties. These functionalities include billing, monitoring, controlling, predicting and planning energy usage and production. In a power plant, energy usage data is required to meet the energy demands, smart meters help realize this in a cost-efficient manner.

Smart grid deployments are very data intensive, from one way meter reading to demand response to real time pricing application, the data exchange between the utility center and the household should be properly engineered and most importantly secured [1]. Electrical grids are considered as national critical infrastructures as they play a vital role in modern society. The failure of a grid can incur huge losses, leading to catastrophe. The wide application of ICT for smart grid has created a massive dependence on its information infrastructure, introducing new kinds of vulnerabilities in the power network [2]:

- Data theft and manipulation: the energy usage readings and other sensitive customer information provided by the smart meter is at risk of being manipulated or being accessed by unauthorized parties.
- Information and communication infrastructure: the smart meters are connected to the Internet to provide data to energy providers and customers. As a result of this the smart grid is prone to traditional attacks on hardware, software and protocols.

Cyber-security for critical infrastructure such as smart grid is a very concerning issue because of emerging cyber-threats and security incidents targeting critical infrastructures all over the world. This article deals with analyzing the vulnerabilities introduced in the smart grid due to the IT nature of smart meters. Generally cyber-attacks in electrical grids can be categorized under three categories [3]:

- Attack on the hardware: such as change value in automation devices, remote terminal unit (RTU) and human–machine interface (HMI).
- Attack on software: such as exploiting vulnerabilities in commonly used DNP3 and Modbus protocols.
- Attack on network topology: exploiting network topology vulnerability, such as denial-of-service (DoS) attack, overflowing an RTU with protocol messages, etc.

These cyber-attacks are based on the exploitation of vulnerabilities present in the underlying computer and networking technologies. The attack on smart grids dealt with in this article exploits the vulnerabilities in the present Internet infrastructure. A person, group or customer with malicious intents can attack a network through a number of actions, one of which is distributed denial-of-service (DDoS) attack. DDoS attack exploits numerous attack sources, spread using multiple hosts to launch a coordinated DoS attack against one or more targets which effectively amplifies the attack power and makes defense more complicated. It is estimated that malicious hackers launch more than 7000 DDoS attacks each day.

The aim of the article is to study the impact of large-scale DDoS attack on the information and communication infrastructure of smart grid AMI network through a network simulation tool called *NeSSi*^{2} [4].

The rest of this article is organized as follows. In Sect. 2, we investigate related work and give some background information. In Sect. 3 we describe the simulation setup. Section 4 discusses the simulation results and discussion. Finally, the conclusion is presented in Sect. 5 to summarize the work.

2 Related Work

According to [5] a recent worldwide poll found that the cyber-attacks increasingly pose a threat to national energy and communication systems. Cyber-security must address not only deliberate attacks, for example from disgruntled employees, industrial espionages, and terrorists, but also accidental compromises of the cyber infrastructure due to user negligence, user errors, equipment failure, and natural disasters. Vulnerabilities may allow an attacker to penetrate a system, get access to a control center, and modify load conditions to destabilize a critical infrastructure in unpredictable ways leading to serious results, for example brownout or even catastrophic blackout [6]. In addition, cyber-security issues may also result in a breach of customer privacy and unpredicted economic losses in the electricity market.

A lot of research work has been carried on smart grids and their security. This section covers a few of those.

2.1 Advanced Metering Infrastructure

Currently, there is no standardized process for the smart grid. Work done in [7] and [8] focuses at a global level whereas [2] is primarily based on the current standards in Germany (Europe). For the ease of understanding, we have put forth a simple overview of the smart metering infrastructure in Fig. 1 that will be used in the study.

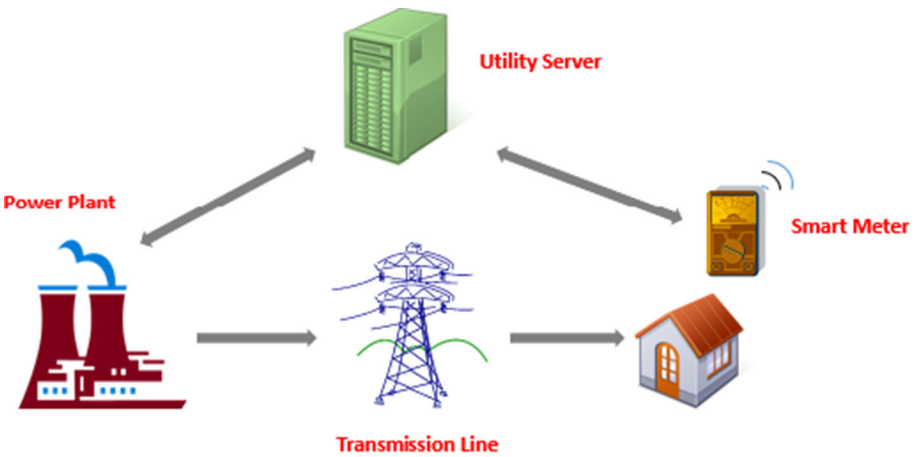


Fig. 1 Advanced metering infrastructure

- *Smart Meter* It is an electronic device with estimated lifetime of several decades which records consumption of electric energy in regular intervals of time and communicates that information back to the utility server. Smart meters are different from conventional electric meters, they enable two-way communication between the meter and the utility server. Smart meters gather data for remote reporting (on-demand and periodic), which is used by the utility server for billing and consumption monitoring purposes.
- *Utility Server* The utility server is housed in the control center. It is in direct communication with the source of generation as well as the consumption units. The server feeds the power generator and the user with live consumption data. This data is finally used at the site of generation to keep track of the energy requirements and by the energy providers for billing. There are no specifications available for the utility server, only the interfaces are specified. The protocols which are used for this are Smart Message Language (SML) for connecting the utility server with Multi Utility communication (MUC) and EDIFACT/MSCONS for billing [2].

2.2 Smart Grid Security

"Where roll-out of smart meters is assessed positively, at least 80 % of consumers shall be equipped with intelligent metering systems by 2020" [9]. With the European Parliament preparing to install smart meters in every home, it becomes even more important that the security of the smart grid is up to the mark.

The most serious threats related to the privacy deterioration of smart grid consumers include [10]:

- Cyber-attack and intrusion
- Identity theft
- Tracking and observing the behavioral patterns of the consumers and the appliances being used
- Real time spying and surveillance

A recent study by Baker et al. [11] highlighted that nearly 80 % of electrical enterprises in 14 countries were victims of large-scale DDoS attacks. Nearly 25 % of the executives who were part of the study reported extortion through threatened or realized cyber-attacks. This was a 20 % increase as compared to the year before. Smart meters will be deployed on a large-scale in a short time and the study emphasizes the critical issue regarding the security of such systems.

Several schemes have been proposed to implement smart grid privacy, some of the schemes are: Anonymous Credential, 3rd Party Escrow Architecture, Load Signature Moderation (LSM), ElecPrivacy, Smart Energy Gateway (SEG) and Privacy preserving Authentication [12]. The study in [13] focused on comparing these proposed approaches and architectures aimed at protecting the privacy of smart grid users.

2.3 Denial-of-Service (DoS) Attack

In this article we will look at one of the conventional cyber-attacks: distributed denial-of-service (DDoS). In contrast to a classic DoS attack that uses a single attack source, DDoS attacks exploit numerous attack sources, spread using multiple hosts, which effectively amplifies the attack power and makes defense more complicated.

The attack on smart grids dealt with in this article exploits the vulnerabilities in the present Internet infrastructure design, which focuses on how to effectively move packets from the source to the destination, malicious or not. The design follows the end-to-end paradigm: the intermediate network provides the best-effort packet forwarding service. The end-to-end paradigm pushes the complexity to end hosts, leaving the intermediate network simple and optimized for packet forwarding. The Internet is not design to police traffic. If one party in two-way communication (source or destination) misbehaves, it can do arbitrary damage to its peer [14].

A typical DDoS attack is externally engineered with an objective to bring down a large portion or even the whole targeted network. One essential issue of DDoS attack and defense is resource competition; if a defender has sufficient resources to counter a DDoS attack, then the attack will be unsuccessful, and vice versa. Recent researches [15] have corrected a long held belief that hackers can easily compromise as many computers as they want. Due to the anti-virus and anti-malware efforts and software, the number of active bots a bot-master can manipulate is constrained to hundreds or a few thousand, even though the number of bot footprints may be much larger.

DDoS attacks can be categorized into two groups: flooding attacks and vulnerability attacks [16].

Flooding attacks SYN flooding [17] and Internet control message protocol (ICMP) flooding are the two of the most popular DDoS flooding attacks. SYN flooding exploits the weaknesses in the Transmission Control Protocol (TCP). SYN packet in TCP is required to establish a connection between any two hosts. It is a request sent by the host to make a connection. Attackers send SYN packets to the ports that are in the 'Listening' state in the target host, these packets have a source address that does not represent the actual host. The target responds with a SYN or ACK packet addressed to the source address in the SYN packet that was received. As the system does not exist and the source address was invalid, the target keeps waiting for a packet acknowledgment to complete the connection process. The allocation of resources by the target in response to these malicious packets leads to a DDoS attack. ICMP flooding exploits configuration errors on the network devices involved. It lets packets to be sent to a network via broadcast address, which were to be sent to a specific host. The attacker sends a large number of IP packets with an invalid source address. This leads to network bandwidth drainage, causing legitimate packets to be blocked. There is also User Datagram Protocol (UDP) flood attack which exploits the connectionless TCP/IP stack protocol to generate a DDoS attack. Using UDP for DoS attacks is not as straightforward as with TCP. A UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a destination host and forcing the destination host to send a large number of ICMP packets.

Vulnerability attacks In this attack, malicious packets exploit network protocol or application fault that exists at the target network. The malicious packets exploit vulnerable software installed at the target hosts, triggering excessive CPU utilization, increasing memory demand, halting the hosts' operation, or other general system braking [16]. Vulnerabilities may allow an attacker to penetrate a system, get access to a control center, and modify load conditions to destabilize a critical infrastructure in unpredictable ways leading to serious results or disaster, for example brownout or even catastrophic blackout [6]. The vulnerability attack can be usually mitigated by implementing regular patching.

In reality, DDoS attack is easily performed by open-source DDoS attack tools such as Low Orbit Ion Cannon (LOIC) or High Orbit Ion Cannon (HOIC). LOIC had been one of the favorite DDoS tools used by Anonymous and other hacker groups. LOIC sends out multiple simultaneous requests for a web page that is unlikely to exist on the target site. It

floods the server with TCP or UDP packets with the intention of disrupting the service of a particular host. Attackers often use Twitter to co-ordinate its DDoS attacks. Due to its popularity, LOIC has been ported to Java and Web based versions. HOIC is considered as an upgraded version of LOIC, it sends high-speed multi-threaded HTTP flood that is able to flood up to 256 websites at once simultaneously. To prevent firewall detection, HOIC targets sub-pages, sends multiple fake users requests to multiple pages within a domain, the welcome pages, the help pages, and anything else a target site has to offer. It is reported that as little as 30–50 attackers equipped with HOIC can cause a significant damage to the target website.

2.4 NeSSi^2

NeSSi^2 is an agent-based simulation environment that provides telecommunication network simulation capabilities with an extensive support to evaluate security solutions such as IDS (Intrusion Detection System) [4]. In contrast to other popular network simulators, such as ns-2 [18], ns-3 [19] or OMNeT++ [20], *NeSSi*^{2} provides a comprehensive detection application programming interface (API) for the integration and evaluation of IDS. Special attack scenarios are relatively easy to simulate and study using *NeSSi*^{2}. *NeSSi*^{2} also provides methods to simulate smart grid networks by supporting both IP and energy networks.

NeSSi^2 is built upon the JIAC (Java-based Intelligent Agent Component ware) framework [21], a service centric agent-framework. All entities, i.e. both IP and energy based are simulated using JIAC agents. Depending on the configuration and the hardware characteristics, each agent simulates one or more nodes (IP/Energy entities).

3 Simulation Design

To evaluate and analyze the effect of a DDoS attack on the smart grid we setup a simulation scenario using *NeSSi*^{2}.

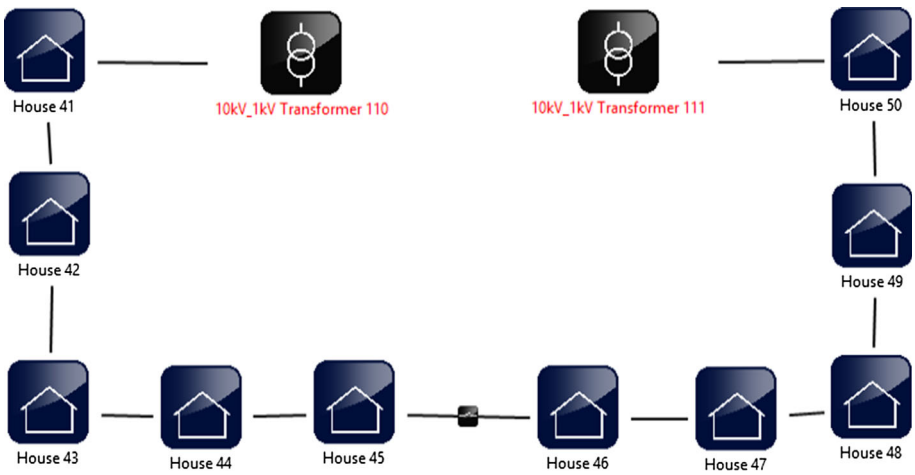


Fig. 2 Energy subnet for smart grid with open ring topology

In our simulation scenario, we simulate a UDP (User Datagram Protocol) storm DDoS attack. We use multiple hosts to send a large number of UDP packets to random ports on a destination host. As a result, the destination host will:

- Check for the application listening at that port;
- See that no application listens at that port;
- Reply with an ICMP Destination Unreachable packet.

Thus, for a large number of UDP packets, the victimized system will be forced into sending a large number of ICMP packets, eventually leading it to be unreachable by other clients. The attacker may also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach them, and anonymizing their network location(s).

In order to mimic a real smart grid environment undergoing a UDP storm attack, we need to federate both IP network and energy network. The topology for both networks is as follows:

Energy Network To make the energy network topology replicate a real life energy network we have taken an open ring topology as it is commonly deployed in larger cities like Glasgow or Berlin [2]. In this topology when there is a fault, the defective part can be isolated by using switches [2]. The network consists of five low voltage sub networks of 1 kV each. Each subnet has an open ring topology as shown in Fig. 2.

Each subnet consists of 10 households with the application Smart Home Consumer running on each house. A total of 50 houses which are simulating energy demands for 250 people in the winter are used. This is done to keep a balance between granularity and the network size. The source of energy is a wind farm running a wind farm application, which is a common scenario for a country like Scotland. Compared to other energy sources, wind energy has clear advantages such as being environment friendly, causing no pollution and having a minimal environmental impact. It is also the most mature and the most utility-scale ready alternative from all the renewable energy solutions [22]. In our simulation, the

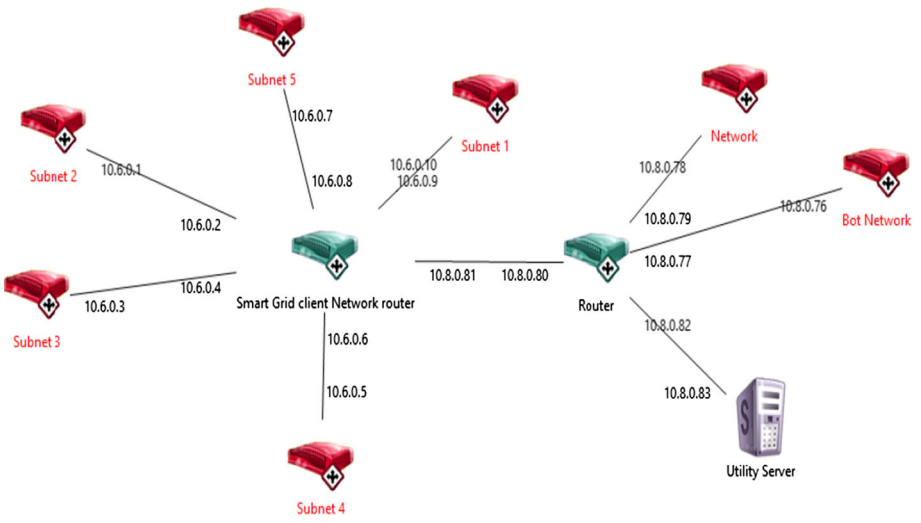


Fig. 3 IP network topology

external supply connecting the source of energy and the subnets utilizes a swing bus and line failure application to analyze the power mismatch between production and consumption and simulate the effects of the attack on the energy network.

IP Network The IP network is similar to the energy network. As depicted in Fig. 3, it consists of five sub-networks with 10 clients in each to simulate the telecommunication part of the smart grid. Each client is mapped to a consumer entity in the energy network. All the five subnets are connected to the utility server, which is responsible for the collection of data from the clients. The utility server is connected to the Internet for billing purposes and is mapped to the power plant. To demonstrate the attack on the utility server, it is connected to a bot network (botnet) (see Fig. 4) which consists of bots, i.e. devices which are used by an attacker for malicious activity. Botnets are often used as the tools to perform DDoS attacks due to the anonymity it provides the attacker as well as the ability to achieve high volumes of traffic with minimal commands being sent. As defined by [4], a botnet is, "a collection of software robots, or bots, which run autonomously and automatically. They run on groups of zombie computers controlled remotely by attackers."

These "bots" are a source of "capability" that aids an attacker in his or her endeavor to perform malicious activity. Recently large-scale DDoS attacks are carried out using botnets controlled by a bot-master via command-and-control (C&C) channels. The bots are then programmed and instructed by the bot-master to perform a variety of cyber-attacks, including DDoS attacks.

In our simulation the IP network used three different profiles:

1. *Client* It is used to model the behavior of a smart meter. Runs applications such as echo client, targeted UDP client application and energy-based IP device failure application.
2. *Server* Utilizes the echo server and IP device failure applications.

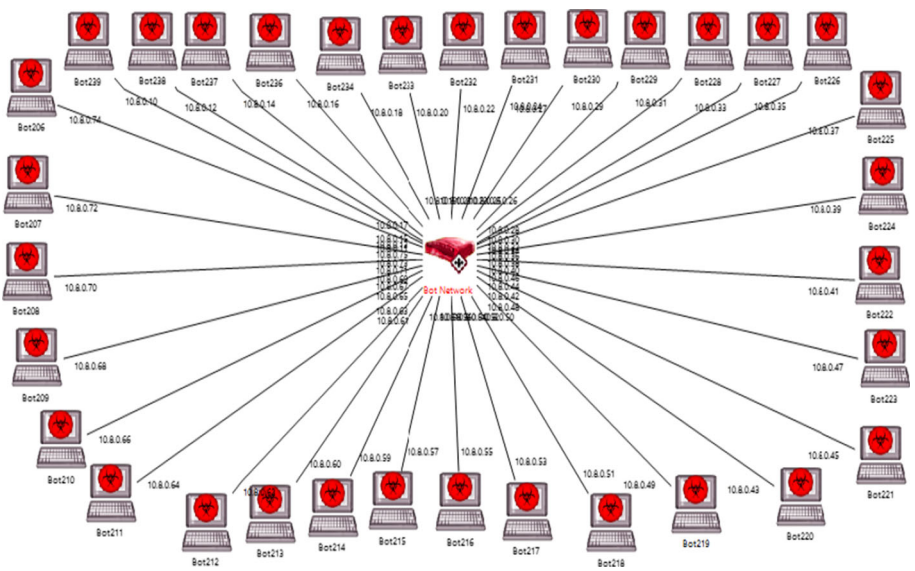


Fig. 4 Bot network

3. *Bot* To simulate the attack, all the bots are loaded with the DDoS application. Distributed UDP storm attack is implemented.

4 Results and Discussion

The federated simulation was run for a duration of 1000 ticks (*tick* is the term for the atomic discrete time unit [4]). The statistics for the utility server and the clients are shown in Figs. 5 and 6, respectively. In Fig. 5, we can see a sudden surge in the number of packets being forwarded to the server at tick 300, signaling a DDoS attack. When the attack continues, the server goes down at tick 500 and starts dropping all incoming packets (see Fig. 5). In the simulation, the Bot network is designed such that it starts flooding the target server with UDP packets at tick 300. After multiple simulation taking different simulation parameters we found that at tick 500, the server was flooded with enough UDP packets, activating the IP device failure app and eventually bringing down the server.

Simulation parameters in the DDoS attack simulation scenario are summarized in Table 1.

On the energy network, the energy produced by the power plant is equal to the demand of the electric grid. However, with the failure of the utility server, the power plant has no usage data as a result of which the power plant stops producing electricity.

In the simulation scenario, the Line failure application is used to mimic this. Thus, the whole network is brought down with the energy production and the load at the power plant and the houses falling to zero (see Figs. 7, 8).

The failure of the energy meter at the houses causes the IP based clients to start dropping packets and seize communication with the utility server (see Fig. 6). It is

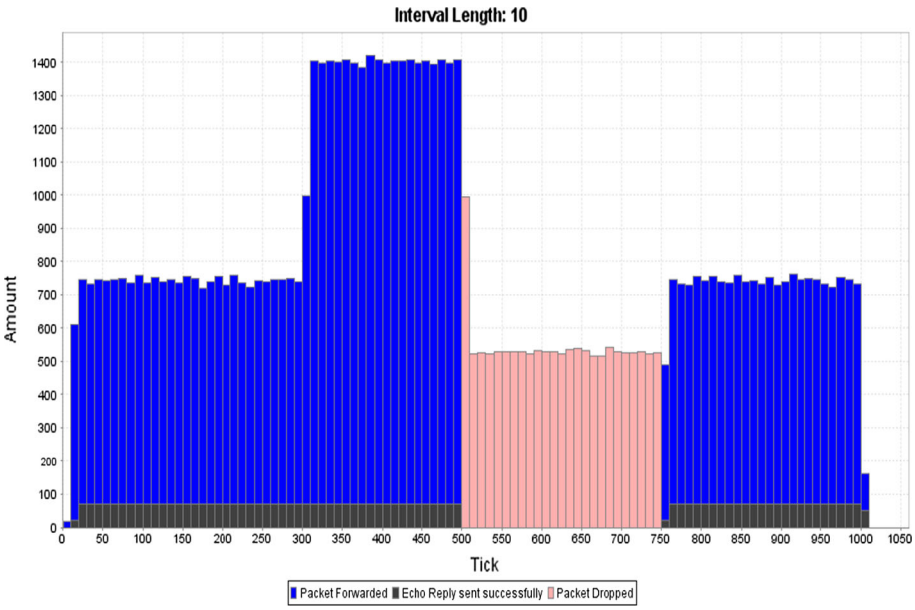


Fig. 5 Packet statistics for the utility server

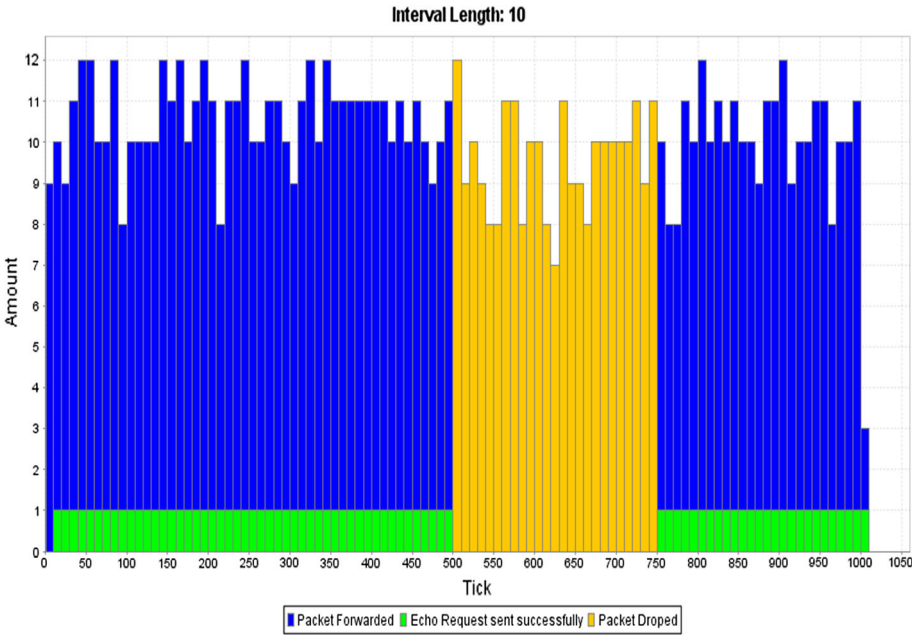


Fig. 6 Packet statistics for each client

Table 1 Simulation parameters

Parameter	Value
Number of botnets	1
Number of bots	33
Number of smart meters	50
Number of houses	50
Number of wind farms	1
Simulation duration (number of ticks)	1000

simulated using the Energy based IP device failure app. This application drops all packets if the voltage of the federated energy device is zero.

In our scenario, the Bot network stopped flooding the server with UDP packets at tick 750. The server as well as the energy network are restores almost immediately (see Figs. 7, 8). As can be seen in Fig. 7, the energy demand immediately after the power outage was quite high (around 19 kW).

An interesting observation in this simulated DDoS attack is that the energy network was not affected during the DDoS attack. The energy network was only affected after the server is down due to the smart grid being brought down.

5 Summary

Electrical power grids are valuable infrastructures and their integration with ICT will play a fundamental role to meet future energy goals and effectively manage the phenomenal

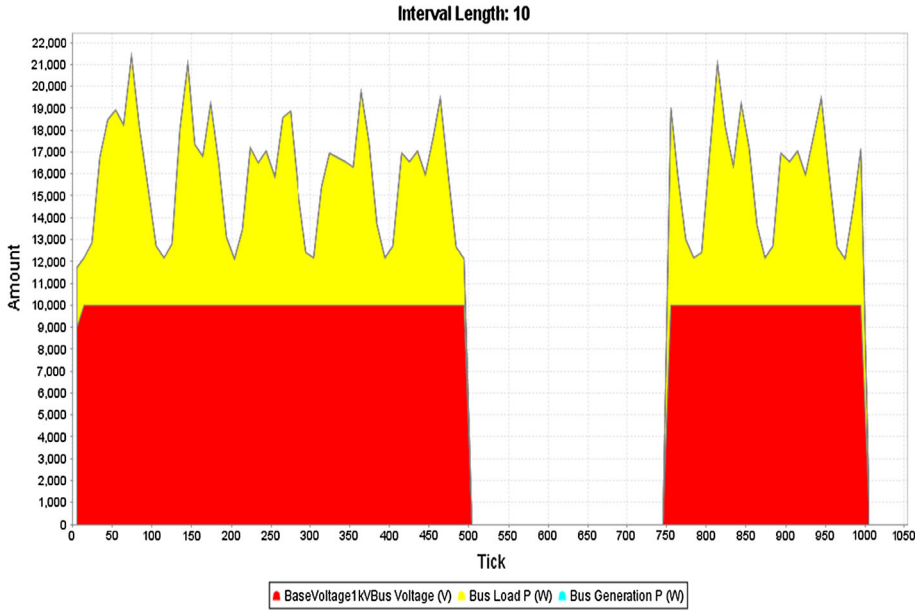


Fig. 7 Load for each house (in Watts)

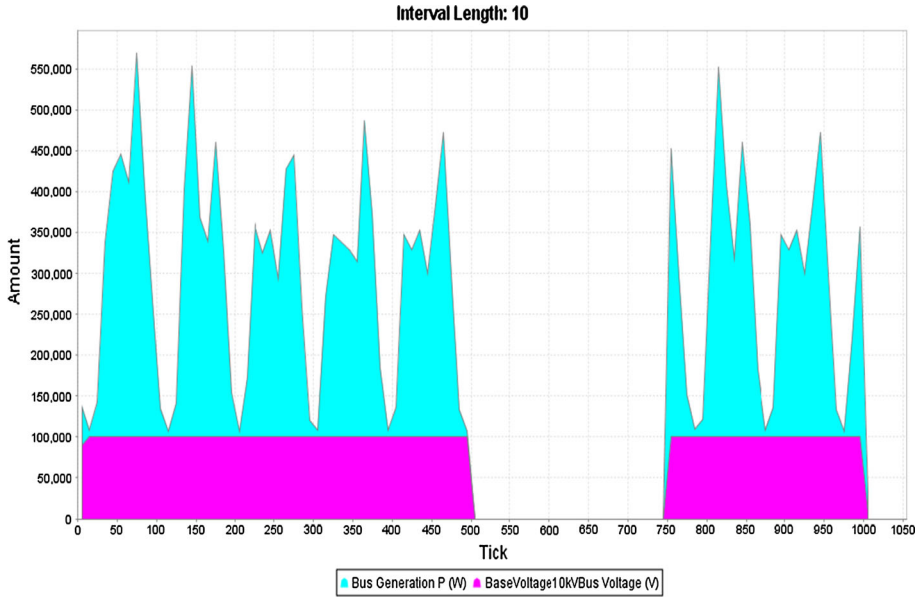


Fig. 8 Power plant generation (in Watts)

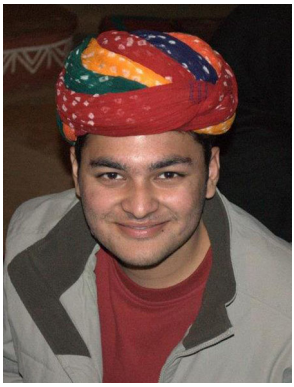
demand and supply of electricity. The article investigated large scale DDoS attack on smart grid AMI network, motivated by a significant increase in cyber-attacks to national critical infrastructure.

The impact of DDoS attack on critical infrastructure availability has been simulated and evaluated. It is clear from the simulation results that the smart grid is highly vulnerable to various types of cyber-attacks, such as DDoS. The simulation results using $NeSSi^2$ show how the whole electrical grid system was successfully brought down by the simulated large-scale DDoS attack. The wide application of ICT for smart grid has created a massive dependence on its information infrastructure, introducing new kinds of vulnerabilities in the power network. The failure of a grid can incur huge losses leading to catastrophe. In case, the smart grid covers critical infrastructure such as an air traffic control center, the effects can be disastrous. With the transformation of the conventional electric grid to a smarter one, steps need to be taken to ensure security is properly planned and in place to ensure a smooth working of the electrical power systems. Future work should focus on how to mitigate and prevent similar cyber-attacks, such as DDoS attacks by applying some mechanism, such as intrusion detection and prevention systems within the above smart grid simulation environment.

References

1. Farquharson, J., Wang, A., & Howard, J. (2012) Smart grid cyber security and substation network security. In *Innovative smart grid technologies* (*ISGT*), *2012 IEEE PES*, (pp. 1–5).
2. Chinnow, J. et al. (2011) A simulation framework for smart meter security evaluation. In *2011 IEEE international conference on smart measurements for future grids* (*SMFG*) (pp. 1–9).
3. Dong, W. et al. (2011) Protecting smart grid automation systems against cyber attacks. In *IEEE transactions on, smart grid* (Vol. 2, pp. 782–795).
4. Schmidt, S., et al. (2010). Application-level simulation for network security. *Simulation, 86*, 311–330.
5. Pearson, I. L. G. (2011). Smart grid cyber security for Europe. *Energy Policy, 39*, 5211–5218.
6. Dollen, D. V. (2009). *Report to NIST on smart grid interoperability standards roadmap*. Palo Alto, CA: Electric Power Research Institute (EPRI).
7. Wang, J., & Leung, V. C. M. (2011). A survey of technical requirements and consumer application standards for IP-based smart grid AMI network. In *2011 International conference on*, *information networking* (*ICOIN*) (pp. 114–119).
8. De Craemer, K., & Deconinck, G. (2010). Analysis of state-of-the-art smart metering communication standards. In *Proceedings of the 5th young researchers symposium*.
9. EC. (2009). Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rule for the internal market in electricity. Journal of the European Union 2009.
10. Efthymiou, C., Kalogridis, G. (2010) Smart grid privacy via anonymization of smart metering data. In *2010 First IEEE international conference on*, *smart grid communications* (*SmartGridComm*) (pp. 238–243).
11. Baker, S., Filipiak, N., & Timlin, K. (2011, April). In the dark: Crucial industries confront cyber-attacks. In *McAfee 2nd annual critical infrastructure protection report*. http://www.mcafee.com/cip.
12. Siddiqui, F et al. (2012) Smart grid privacy: Issues and solutions. In *2012 21st international conference on*, *computer communications and networks* (*ICCCN*) (pp. 1–5).
13. Zeadally, S., et al. (2013). Towards privacy protection in smart grid. *Wireless Personal Communications, 73*, 23–50.
14. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Computer Communication Review, 34*, 39–53.
15. Rajab, M. A. et al. (2007) My botnet is bigger than yours (maybe, better than yours): Why size estimates remain challenging. In *Proceedings of the 1st USENIX workshop on hot topics in understanding botnets*. Cambridge.
16. Carl, G., et al. (2006). Denial-of-service attack-detection techniques. *Internet Computing, IEEE, 10*, 82–89.
17. CERT. (1996). *CERT advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks*. http://www.cert.org/advisories/CA-1996-21.html.
18. ns-2. (2013). *The network simulator—ns-2*. http://www.isi.edu/nsnam/ns/. December 10, 2013.

19. Riley, G., & Henderson, T. (2010). The ns-3 network simulator. In K. Wehrle, et al. (Eds.), *Modeling and tools for network simulation* (pp. 15–34). Berlin: Springer.
20. Varga, A., & Hornig, R. (2008) An overview of the OMNeT++ simulation environment. In *1st international conference on simulation tools and techniques for communications*, *networks and systems and workshops* (pp. 1–10). Marseille.
21. Hirsch, B., Konnerth, T., & Heßler, A. (2009) Merging agents and services: The JIAC agent platform. In *Multi-agent programming* (pp. 159–185). Springer: Berlin.
22. Glinkowski, M., Hou, J., & Rackliffe, G. (2011). Advances in wind energy technologies in the context of smart grid. *Proceedings of the IEEE, 99*, 1083–1097.



Satin Asri is a final year undergraduate student in the Department of Computer science and Engineering at Manipal Institute of Technology, India. His research interests includes network and information security, risk management and internet of things.

Bernardi Pranggono is a lecturer and the programme leader for M.Sc IT Security and M.Sc Digital Forensics at the Department of Computer, Communications and Interactive Systems, Glasgow Caledonian University (GCU). Prior to joining GCU he was a post-doctoral researcher at the Queen's University Belfast, where he worked on a range of EU and EPSRC projects in the Centre for Secure Information Technologies (CSIT). Previously, he held industrial positions at Accenture, Telstra, and PricewaterhouseCoopers. Dr. Pranggono received his B.Eng degree in electronics and telecommunication engineering from Waseda University, Japan, M.DigComms degree in digital communications from Monash University, Australia and Ph.D. degree in electronics and electrical engineering from the University of Leeds, UK. His current research interests include network security, optical networking, cloud computing, and green ICT. Dr. Pranggono has co-authored over two-dozen papers in leading international conferences and journals, and contributed to three book chapters. He has served as Vice-Chair and Technical Program Committee member in numerous international conferences, such as IEEE HPCC and GLOBECOM. He also serves as referee of some renowned journals and conferences, such as IEEE Transaction on Industrial Informatics, IEEE Transaction on Power Delivery, IEEE Communication Magazine, IEEE Computer, IEEE GLOBECOM, IEEE ICC, Elsevier Optical Switching and Networking, etc.