A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures

Alvin Huseinovic, Sasa Mrdovic, Kemal Bicakci, and Suleyman Uludag

Abstract—**The scope, scale, and intensity of real, as well as potential, attacks on the Smart Grid have been increasing and thus gaining more attention. An important component of the Smart Grid cybersecurity efforts addresses the availability and access to the power and related information and communications infrastructures. In this paper, we provide a holistic and methodical presentation of taxonomies and solutions for DoS attacks in the Smart Grid. The emerging threats of cybertattacks are raising serious concerns for many critical infrastructures. In this regards, The scope, scale, and intensity of real as well as potential attacks on the Smart Grid are on the rise and with devastating consequences. An important component of Smart Grid cybersecurity efforts addresses the availability and access to the power and related information and communications infrastructures. In this paper, a holistic and methodical presentation of taxonomies and solution for DoS attacks in the Smart Grid is presented.**

Keywords — Denial-of-Service attacks, cyber-physical systems, smart grid security

I. Introduction

The power grid is considered to be the largest machine in the world. Recently, worldwide initiatives have started upgrading the power grid infrastructure to the Smart Grid (SG). This vast upgrade involves integration of a variety of digital, computing, communications, and industrial control systems and technologies into a modernized and advanced power grid. A key element of the SG effort is in the incorporation of the bidirectional flow of power (for distributed and renewable energy sources) as well as the two- way communications and control capabilities. Even before the SG initiatives, the nature of the power grid was vulnerable to malfunction that could disturb its precarious equilibrium and its applications for reliability purposes. Both top-down governmental and bottom-up-societal trends to incorporate more distributed resources, including renewables, exacerbate the known power grid deficiencies and make it more vulnerable to deliberate attacks. For example, the number of smart meters show (Figure 1) a quadratic increase in worldwide deployment, which in turn increases the attack vectors with the same proportion. As a result, a critical need emerges to address a variety of security and privacy related challenges.

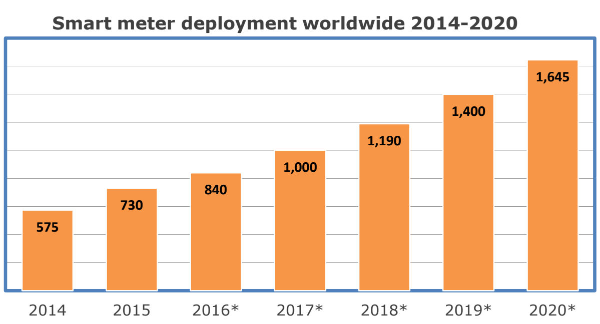

Fig. 1. Number of smart meters (electricity, gas & water) worldwide from 2014 to 2020 (in millions), real data up to 2015, and then forecast thereafter.

Cybersecurity becomes an indispensable component and key enabler for the successful transformation from the electric power grid of yesterday into the SG of the future. The essential nature of the SG cybersecurity spans availability, integrity, and confidentiality of computing, communications, and/or control devices from intentional or accidental harm and damage. Out of so many other real incidents, in December 2015 in Ukraine, cyber attacks were directly responsible for power outages [1]. These attacks as well as other potential attack vectors on power grid [2] have revealed tenuous vulnerabilities of systems, components, and people in both the private and public sectors. There is definitely an imperative to implement and adopt cybersecurity technology, both within the SG and beyond.

Conventionally, *availability*, the target of Denial-of-Service (DoS) attacks, is defined as "ensuring timely and reliable access to and use of information"[3]. However in the context of SG "ensuring access to enough power" should also be considered as part of the definition.

With this expanded definition, availability is regarded as a crucial security objective for SG [3]. DoS attacks disrupting the Internet traffic have already cost billions of dollars worldwide. With the increasing connectedness of grid systems, a DoS attack to the infrastructure causing a major power failure becomes quite possible and could be undoubtedly more harmful and costly. This is because in modern society electricity is a utility we depend on mightily not only for communication but also for many other life-critical functions.

In this work, we present a structured, methodical, holistic, and comprehensive view of the *availability* dimension of the SG cybersecurity by proposing a taxonomy of denial-of-service attacks and a very high-level glimpse (due to space limitation) of potential solutions. To the best of our knowledge, a comprehensive study about DoS attacks and solutions on the SG does not exist in the literature. Hereby, we would like to draw the various research communities' attentions to these important cybersecurity issues to draw more concerted efforts towards more viable and readily available solutions.

The rest of this paper is organized as follows: We pro-

A. Huseinovic and S. Mrdovic are with the Faculty of EE, U. of Sarajevo, Bosnia & Herzegovina, email: {ahuseinovic,sasa.mrdovic}@etf.unsa.ba.

K. Bicakci is with the Dept. of Comp. Eng., TOBB U. of Economics and Technology, Ankara, Turkey e-mail: bicakci@etu.edu.tr.

Suleyman Uludag is with the Dept. of Computer Science at the U. of Michigan - Flint, email: uludag@umich.edu.

vide a taxonomy of DoS attacks on the SG from multiple perspectives in Section II with brief discussions of each for brevity. Section III follows it up with a synopsis discussion of some potential solution approaches without details due to space limitation but with a summarizing comparative table. Concluding remarks are provided in Section IV.

II. Smart Grid DoS Attacks

In this section, we summarize five different classifications of DoS attacks on the SG.

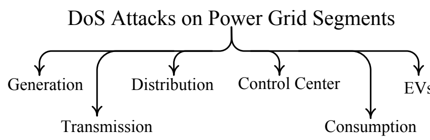

Fig. 2. Spatial classification of DoS attacks on the SG.

First classification may be stated in the terms of the spatial dimension, as shown in Fig. 2. DoS attacks may target all the segments of the SG, from generation, transmission, distribution, and consumption to control centers and Electric Vehicles (EVs) charging/discharging infrastructure.

The SG comprises bidirectional transmission of both power and information. From the communications perspective, the attacks may originate at different layers, from physical and data link layers all the way to the network, transport, and application layers, as shown in Fig. 3.

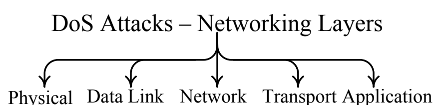

Fig. 3. SG DoS attacks in terms of communications layers.

A DoS attack may exploit vulnerabilities with respect to the commonly used communications protocols peculiar to the utility companies, as shown in Figure 4. IEC 61850

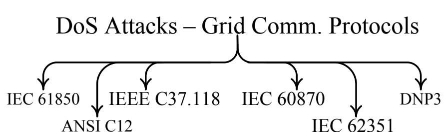

Fig. 4. Smart Grid DoS attacks in terms of the major power grid communications protocols.

is a networking protocol for substation automation. Besides running on top of TCP/IP, and hence inheriting all the DoS vulnerabilities from the Internet domain, possible DoS attacks exploiting two of IEC 61850's protocols (GOOSE and SV) are reported in [4]. A general discussion of security threats with DoS focus can be found in [5], [6]. ANSI C12.22/IEEE 1703 defines a communications protocol for Advanced Metering Infrastructure (AMI). A distributed DoS attack scenario is presented in [7], [8] for C12.22 service. IEEE C37.118 is the networking protocol for the Phasor Measurement Unit (PMU) data. DoS attacks on C37.118 are studied in [9], [10]. The IEC 60870 family of standards cover communications for SCADA (supervisory control and data acquisition). [11] discusses potential DoS attacks. Simulation-based analysis of DoS attacks from the IEC 62351's perspective is presented in [11]. Finally, DNP3, an alternative protocol for SCADA used by utility companies, has its own set of DoS related problems, as detailed in [12].

Another taxonomy may be analyzed by means of the major power grid applications, as depicted in Figure 5. As the cru-

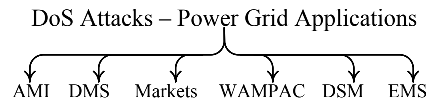

Fig. 5. Smart Grid DoS attacks in terms of the major power grid applications.

cial application of the SG, Advanced Metering Infrastructure (AMI) is the last mile where smart meter to the utility bidirectional communication and data transfers take place. Several studies highlight the DoS attacks in AMI [13], [14], [15], [16]. An example DoS attack on an AMI network is depicted in Fig. 6 [7]. An integral component of SG is the Distribution

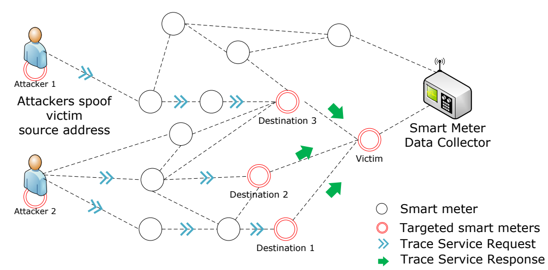

Fig. 6. An attack scenario on the AMI [7].

Management System (DMS) that is in charge of monitoring, protection, control, and optimization of distribution assets. [14], [17] introduce load frequency disturbance as a result of a DoS attack and load altering attack is discussed in [18]. DoS attacks to energy markets, especially pricing, are covered in [6], [19]. Wide Area Monitoring, Protection, and Control Systems (WAMPAC) [20] are also prone to DoS attacks, as described in [10], [21]. Demand Side Management (DSM) involves techniques to maintain the load and supply equilibrium from the demand side. DoS potentials are presented in [6], [18]. The North American Electric Reliability Corporation (NERC)'s Cyber Attack Task Force from 2012 outlines the risk of DoS on Energy Management System (EMS) with targeted attack scenario is detailed in [22].

A final taxonomy of the DoS attacks in terms of the *techniques* employed is given in Figure 7. We posit seven

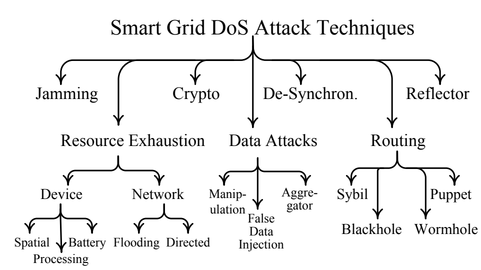

Fig. 7. A taxonomy of the DoS attack techniques in the Smart Grid.

different main categories of techniques that a DoS attack may utilize: Signal jamming at the physical layer may be initiated to deny, delay, or degrade information or electricity service [5], [14] [23]-[25]. Resource exhaustion DoS attacks may target a device or a network. For the former [11],

[12], [26], spatial types are for depleting some dimension of memory while processing and battery target the computing and power resources, respectively. For the latter [6], [15], [27], flooding is an indiscriminate transmission of traffic to saturate the bandwidth while the directed is a more targeted transfer of deluge of data. One cryptographic DoS attack scenario is explained in [28] where a Message Authentication Code used to prevent data corruption may be exploited to trigger a DoS attack. Data manipulation may be used as a stepping stone to launch DoS attacks [2], [18], [19]. While the goal of the false data injection attacks [6] may be on integrity, it may also be easily used as a DoS tool [2], [29]. Data aggregation is an important part of the data collection subsystem of the SG. A typical hierarchical data collection by means of data aggregators is a boon for initiating a DoS attack [6], [12], [14], [16], [30]. Many applications of the SG is highly sensitive to the timeliness of the data and the transactions. De-synchronization attacks can be utilized as another form of DoS. SG involves bidirectional data transfers and routing, in this respect, becomes an important mechanism and attractive target for DoS attacks. Typical routing-based DoS attacks are directly applicable for the SG domain, such as the sybil, wormhole, blackhole, and puppet attacks. Reflector attack involves spoofed requests to a set of servers that will in return send their replies to the target node having the spoofed address. In [7], ANSI C12.22 protocol is shown to be vulnerable to a distributed DoS attack in which a number of compromised smart meters generate trace requests carrying the source address of a victim machine.

III. Discussion on Counterbalancing

Table I shows a preliminary synopsis of potential remedial approaches for the aforementioned attack techniques. Due to the page limit, we discuss these briefly below.

Filtering could be used against certain jamming attacks as demonstrated in [31]. Filtering is the de-facto standard mechanism against resource exhaustion attacks. Crypto attacks could not be avoided by filtering since firewalls do not have the capability to inspect packets based on their cryptographic properties. Although not specifically discussed in the literature, filtering could be used against de-synchronization attacks. Perimeter defense is helpless against most routing attacks but host-based filtering combined with exchanged alarm messages [31] could prevent malicious nodes to participate in the routing protocol. Finally, reflector attacks could be blocked by egress filtering implemented on a perimeter firewall if the attacker and the victim are not in the same network.

Although IDS/IPS (Intrusion Detection/Prevention System) is regarded as a more sophisticated defense mechanism, it is similar to firewalls in the sense that the kind of DoS attacks it could be used against are broadly similar. The key difference is the fact that some attacks could be avoided by an IDS/IPS but not by firewalls.

If DoS traffic could not be distinguished from the legitimate one, rate limiting may be the only mitigation option. For instance, the rate of jamming pertaining to a single source could be reduced. However, especially in time-critical applications it seems unlikely that rate-limiting, by itself, could be sufficient.

We define "jamming" as attacks only in the physical layer and thus cryptography authentication does not help. Crypto-attacks may not be completely avoided by cryptographic authentication but may be limited using lightweight cryptographic primitives. Most of the time, de-synchronization, routing and reflector attacks are initiated as a result of spoofing. Cryptographic authentication is the de-facto solution against spoofing. It works unless the devices are compromised. Although not specifically designed for the SG, coordinated and uncoordinated protocols can be used against jamming [31]. Protocol solutions could be applied against all SG DoS attacks while secure communication protocol design is a challenge. Against jamming attacks, use of wired instead of wireless communication is an extreme example for an architectural solution. The network architecture is not relevant against crypto attacks. Some of the reflector attacks could be addressed by a logical re-architecture [47].

Honeypots are generic DoS countermeasures. However, it could not be the only solution since the attacker could always attack the real target at the same time.

Device solutions prevent the attackers from compromising SG devices. They are not effective against jamming and crypto attacks since these attacks could be performed using external devices. Device solutions and cryptographic authentication complement each other and provide a perfect solution against many different kinds of DoS attacks.

The ability to listen nearby wireless communication by special "watchdog" nodes is proven useful against some other types of DoS attacks including routing and reflector attacks.

If we could model the effects of crypto attacks and reflector attacks at a system level, system-theoretic solutions could even be applied to these sophisticated cyber attacks.

IV. Conclusion

In this review study, we have focused on an important dimension of the SG cybersecurity: DoS attacks and solutions. DoS vulnerabilities for the SG has been expanding with ever increasing severity of successful compromises. The literature does not seem to have any other study as presented here in terms of the scope and coverage.

References

[1] M. J. Assante, "Confirmation of a coordinated attack on the ukrainian power grid," Jan 2016, https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.

[2] S. Goel and Y. Hong, *Smart Grid Security*. London: Springer London, 2015, ch. Security C, pp. 1–39.

[3] Victoria Y. Pillitteri and Tanya L. Brewer, "NISTIR 7628 Revision 1, Guidelines for Smart Grid Cybersecurity," Smart Grid Interoperability Panel (SGIP), Smart Grid Cybersecurity Committee, p. 668, sep 2014.

[4] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *ISGT 2014*. IEEE, feb 2014, pp. 1–5.

[5] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 4, pp. 998–1010, 2012.

[6] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[7] D. Jin, Y. Zheng, H. Zhu, D. M. Nicol, and L. Winterrowd, "Virtual Time Integration of Emulation and Parallel Simulation," in *ACM/IEEE PADS*, jul 2012, pp. 201–210.

TABLE I

A COMPARISON OF DOS ATTACKS VERSUS PROPOSED SOLUTIONS. ○ : NOT VIABLE, ◐ : PARTIALLY VIABLE, ◗: COMPLEMENTARY, ● : VIABLE.

Solutions	**DoS Attacks**						
	Jamming	Res. Exhaus.	Crypto	Data	De-Synch.	Routing	Reflector
Filtering	[31]	[10], [31]	○	[31]	●	[31]	◐
IDS/IPS	[13]	[4], [11], [13], [32]	○	[4], [10], [32]	[4], [10]	[13]	●
Rate Limit	◗	●	◗	◗	◗	○	◗
Crypto. Auth.	○	[33], [34], [35]	◐	[18], [36]	◐	◐	◐
Protocol	●	[35], [37]	[28]	[14], [29], [30], [35], [37]	●	[15], [21]	●
Architectural	●	[38], [39]	○	[39]	[39]	[39]	◐
Honeypots	◗	[40]	◗	◗	◗	◗	◗
Device	○	[41], [42]	○	[41]	◗	◗	◗
Wireless-specific	[24]	[24], [31]	○	[31]	[24]	◐	◐
System-theoretic	[23], [43], [25]	[44]	◐	[18], [19], [22] [44]-[46]	[20], [44]	[44]	◐

[8] S. Rana, H. Zhu, C. W. Lee, D. M. Nicol, and I. Shin, "The Not-So-Smart Grid: Preliminary work on identifying vulnerabilities in ANSI C12.22," in *IEEE Globecom*, dec 2012, pp. 1514–1519.

[9] T. H. Morris and U. Adhikari, "Cyber security recommendations for wide area monitoring, protection, and control systems," in *2012 IEEE Power and Energy Society General Meeting*. IEEE, jul 2012, pp. 1–6.

[10] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono, P. Brogan, and H. Wang, "Intrusion detection system for network security in synchrophasor systems," in *IET IETICT*, 2013, pp. 246–252.

[11] K. Choi, X. Chen, S. Li, M. Kim, K. Chae, and J. Na, "Intrusion detection of NSM based DoS attacks using data mining in Smart Grid," *Energies*, vol. 5, no. 10, pp. 4091–4109, 2012.

[12] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems," in *Proceedings - Winter Simulation Conference*, 2011, pp. 2614–2626.

[13] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions," in *IEEE SmartGridComm*, oct 2010, pp. 350–355.

[14] W. G. Temple, B. Chen, and N. O. Tippenhauer, "Delay makes a difference: Smart grid resilience under remote meter disconnect attack," in *IEEE SmartGridComm*, oct 2013, pp. 462–467.

[15] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *Journal of Network and Computer Applications*, may 2015.

[16] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cardenas, and J. G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," in *IEEE SmartGridComm*, nov 2012, pp. 395–400.

[17] X. P. Liu and A. El Saddik, "Denial-of-Service (dos) attacks on load frequency control in smart grids," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, feb 2013, pp. 1–6.

[18] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, dec 2011.

[19] Y. Li, R. Wang, P. Wang, D. Niyato, W. Saad, and Z. Han, "Resilient PHEV charging policies under price information attacks," in *IEEE SmartGridComm*, 2012, pp. 389–394.

[20] V. Terzija, G. Valverde, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, "Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80–93, jan 2011.

[21] J. Wei and D. Kundur, "A flocking-based model for DoS-resilient communication routing in smart grid," in *2012 IEEE Global Communications Conference (GLOBECOM)*. IEEE, dec 2012, pp. 3519–3524.

[22] O. Vukovic and G. Dan, "Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks," *IEEE JSAC*, vol. 32, no. 7, pp. 1500–1508, jul 2014.

[23] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact Dynamic Game Strategy for Jamming Attack in Electricity Market," 2015.

[24] Z. Lu, W. Wang, and C. Wang, "Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications," *IEEE Trans. on Mobile Computing*, vol. 13, no. 8, pp. 1746–1759, aug 2014.

[25] H. Li, L. Lai, and R. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," in *2011 45th Annual Conference on Information Sciences and Systems*. IEEE, mar 2011, pp. 1–6.

[26] F. M. Cleveland, "Cyber security issues for Advanced Metering Infrasttructure (AMI)," in *2008 IEEE PES - Conversion and Delivery of Electrical Energy in the 21st Century*. IEEE, jul 2008, pp. 1–5.

[27] S. Asri and B. Pranggono, "Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure," *Wireless Personal Communications*, mar 2015.

[28] V. Kolesnikov and W. Lee, "MAC aggregation protocols resilient to DoS attacks," *Smart Grid Communications,2011 IEEE international conference*, vol. 7, no. 2, pp. 226–231, 2011.

[29] O. Vukovic and G. Dan, "Detection and localization of targeted attacks on fully distributed power system state estimation," in *IEEE SmartGridComm*. IEEE, oct 2013, pp. 390–395.

[30] I. Doh, J. Lim, and K. Chae, "Secure Aggregation and Attack Detection for Smart Grid System," in *2013 16th International Conference on Network-Based Information Systems*. IEEE, sep 2013, pp. 270–275.

[31] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, 2011.

[32] R. Berthier and W. H. Sanders, "Specification-Based Intrusion Detection for Advanced Metering Infrastructures," in *IEEE ISDC*, dec 2011.

[33] D. He, S.-C. Chan, Y. Zhang, M. Guizani, C. Chen, and J. Bu, "An enhanced public key infrastructure to secure smart grid wireless communication networks," *IEEE Network*, vol. 28, pp. 10–16, 2014.

[34] D. Wu and C. Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid," *IEEE Trans. on Smart Grid*, vol. 2, no. 2, jun 2011.

[35] C. Rosinger and M. Uslar, "Smart grid security: Iec 62351," in *Standardization in Smart Grids*. Springer, 2013, pp. 129–146.

[36] R. Anderson and S. Fuloria, "Who Controls the off Switch?" in *IEEE SmartGridComm*, oct 2010, pp. 96–101.

[37] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 1233–1241.

[38] A. Khelil, S. Jeckel, D. Germanus, and N. Suri, "Towards benchmarking of p2p technologies from a scada systems protection perspective," in *Mobile Lightweight Wireless Systems*. Springer, 2010, pp. 400–414.

[39] T. T. Tesfay, J.-P. Hubaux, J.-Y. Le Boudec, and P. Oechslin, "Cyber-secure communication architecture for active power distribution networks," in *ACM Applied Computing*, 2014, pp. 545–552.

[40] D. I. Buza, F. Juhász, G. Miru, M. Félegyházi, and T. Holczer, "Cryplh: Protecting smart energy systems from targeted attacks with a plc honeypot," in *Smart Grid Security*. Springer, 2014, pp. 181–192.

[41] A. J. Paverd and A. P. Martin, "Hardware security for device authentication in the smart grid," in *Smart Grid Security*. Springer, 2013.

[42] S. E. McLaughlin, D. Podkuiko, A. Delozier, S. Miadzvezhanka, and P. McDaniel, "Embedded firmware diversity for smart electric meters." in *HotSec*, 2010.

[43] H. Li and Z. Han, "Manipulating the electricity power market via jamming the price signaling in smart grid," in *2011 IEEE GLOBECOM Workshops (GC Wkshps)*. IEEE, dec 2011, pp. 1168–1172.

[44] M. Parvania, G. Koutsandria, V. Muthukumary, S. Peisert, C. McParland, and A. Scaglione, "Hybrid control network intrusion detection systems for automated power distribution systems," in *IEEE DSN*, 2014.

[45] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[46] S. Li, Y. Yilmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *Smart Grid, IEEE Transactions on*, vol. 6, no. 6, pp. 2725–2735, 2015.

[47] M. Handley and A. Greenhalgh, "Steps towards a dos-resistant internet architecture," in *Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture*. ACM, 2004, pp. 49–56.