2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) | 978-1-6654-3254-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/SMARTGRIDCOMM52983.2022.9961

iCAD: information-Centric network Architecture for DDoS Protection in the Smart Grid

George Torres
Computer Science Department
New Mexico State University
Las Cruces, U.S
gtorresz@nmsu.edu

Sharad Shrestha
Computer Science Department
New Mexico State University
Las Cruces, U.S
sharad@nmsu.edu

Satyajayant Misra
Computer Science Department
New Mexico State University
Las Cruces, U.S.
misra@cs.nmsu.edu

***Abstract*—With the proliferation of differently-abled and heterogeneous devices in the smart grid Denial of Service (DoS) is becoming an even more potent attack vector than it was before. This paper demonstrates the ease with which an adversary can orchestrate DoS and distributed DoS (DDoS) attacks on the grid. We then propose iCAD–an information-centric architecture, which extends the iCAAP architecture proposed by us [8], complete with mitigation strategies built for DoS/DDoS resilience. We discuss our architecture in detail and demonstrate the architecture and the mitigation technique's effectiveness in mitigating DoS/DDoS attacks in the face of significant attack load from the distributed agents.**

***Index Terms*—Denial of Service; Distributed Denial of Service; Named Data Networking; Security; Smart Grid.**

I. Introduction

The smart grid electrical network enables two-way communication between nodes. This two-way communication enables grid devices to operate with real-time feedback for grid control and resilience. While this facilitates several operations, it also introduces a new cyber-physical challenge. An adversary can use mechanisms such as denial of service (DoS) attacks to jam the network communications [11], [17]. DoS is one of the more common and easy to orchestrate network attacks, where the attacker floods the network with spurious requests, thus exhausting the network and computational resources to deprive legitimate users of service. DoS attacks can happen at all layers of the TCP/IP protocol stack [2]. Multiple attackers/agents spread across the network can collude to orchestrate distributed denial of service (DDoS) attacks, which are more destructive. DoS/DDoS forms a potent attack vector. These attacks can be orchestrated to disable network communications, and devices, and also for false data injection. For example, the device disabling attack was performed on December 23, 2015, when the Ukrainian power generation was attacked by the 'Blackenergy' virus, shutting down 30 substations.

DDoS attacks can be divided into three categories: volumetric attack, protocol attack, and application attack. Volumetric attack throttles the network bandwidth as the attackers transmits a huge volume of data. Protocol attack targets Layer 3 and Layer 4 of the network stack throttling the processing capacity of network infrastructure. Application attack targets Layer 7 of the OSI model and consumes excessive disk and memory. In this paper, we focus on volumetric attacks where attackers inject a large number of packets into the network (orders of magnitude more than the network can handle) to overwhelm the network links. A cyber physical analysis is required to investigate the impact of cyber attacks [16]. National Institute of Standards and Technology (NIST) lists confidentiality, integrity, and availability as security goals for smart grids. DDoS attacker challenges the integrity and availability of information as DDoS packets are not legitimate and the attack blocks system resources, thus precluding legitimate users. DoS/DDoS attacks can make the dynamic power system unstable with a steady state errors [9].

Named Data Network (NDN) is a new concept that leverages the Information Centric Networking (ICN) paradigm. NDN satisfies the stringent requirement for smart grid communication [18]. NDN uses expressing naming, inherent multicast, custom forwarding, and built-in security measures [12]. Each router consists of Pending Interest Table (PIT), Forwarding Information Base (FIB), Content Store (CS), and forwarding strategies for interest and data packet forwarding. PIT stores unsatisfied interest that the router has forwarded. FIB is a name prefix-based routing protocol that maps a name to the interface. CS is a cache that stores popular packets. Forwarding strategies define the rules to forward interest and data packets. In [8], [12], [15] authors presented an incremental designed NDN architecture so that it meets the need for smart grid communication.

In NDN the network layer is based on Interest and Response. Thus, the routers are capable of responding independently to requests for data. However, in traditional IP protocol, there is no way for the packets to be distinguished at the router (network layer), hence there is no way to provide specialized treatment to the routers. Data packets are a response to interest

Research partly supported by NSF awards #2148358 (RINGS), #1800088, #2028797, #1914635, EPSCoR Cooperative agreement OIA-1757207; and the US DoE SETO award number DE-EE0008774 grant, and the DOD DEVCOM Analysis Center under Cooperative Agreement Number W911NF-22-2-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

packets. It is difficult to flood a node in NDN because it does not involve talking directly to the host and only deals with content [6]. However, if multiple adversary nodes collude and create a list of nodes generating the most number of traffic, the adversary is likely to find the important nodes in the network.

In this paper, we propose our architecture, iCAD, which is designed for making DDoS attacks extremely difficult. We also demonstrate the efficacy of our architecture by showing how it works in a 2500 bus system that uses an information centric network (NDN) approach network analysis and mitigation approaches. We also investigate the loss and delay in the system due to DDoS attack in the multi-hop network.

Contribution: To summarize our contributions: (i) We present the iCAD architecture, which is a novel architecture for DDoS mitigation in an NDN-based smart grid network. (ii) We created a co-simulation framework where communication between nodes uses the iCAD architecture and the power system is simulated using the OpenDSS simulator. (iii) We propose a mechanism to orchestrate DDoS attack in our network and propose a mitigation approach as part of iCAD. (iv) We demonstrate how DDoS agents can collude and orchestrate a DDoS attack and how our mitigation approach can significantly reduce the impact of the attack.

The rest of the paper is organized as follows. Section II reviews the existing literature on DoS and DDoS attacks, along with the mitigation strategy. We present the iCAD system design in Section III. Experiment setup and results are explained in section IV, and in Section V we draw our conclusion.

II. Related Work

An NDN network, like an IP network, is vulnerable to DoS attack. Attackers could overflow the PITs which prevents them from handling legitimate interests. It is hard to determine the source of the attack since NDN packets do not have source information. In [14] hash table (HT) based lookup algorithm, SipHash, was used for NDN interest forwarding that has an extremely low probability of hash collision. A 2-stage longest prefix match (LPM) algorithm was used with virtual FIB entries. Here, lookup starts with a certain short name prefix and either continue to shorter prefix or restarts from a longer prefix. This design included PIT partitioning for multi-core speedup and an optimized data structure that provides DoS resistance in NDN networks.

Router Statistics and Push-back Mechanism are two countermeasures proposed in [7]. Using router statistics, each router keeps count of the number of interests per outgoing interface and does not send more interest on an interface than its physical limitation. Routers can also limit the number of interests for a particular prefix. In the push-back mechanism, a router throttles interest from a namespace when the PIT threshold for that namespace is reached. This limits the interest for a particular namespace from being forwarded.

Simulation using Matlab/Simulink was used in [9] to investigate the DoS attack on load frequency control (LFC) of smart grid communication channels. An adversary can use a DoS attack to jam the communication channel or by flooding the network traffic to cause congestion in the network, making the power system unstable. [19] analyzed DoS attack on a two-area four-machine power system with a utility-scale photovoltaic (PV) plant. Packet arrival time was used to detect DDoS attacks. If anticipated packets did not arrive on time it is flagged and countermeasures were implemented to replace the missing data. Missing data were replaced by either last received or cellular computational network (CCN) based virtual synchrophasor network (VSN) estimated data. Although the test used real-time synchrophasor test, solar irradiance was not considered.

Poseidon is a method to detect DoS attacks introduced in [4]. Poseidon runs on routers and keeps statistics of namespaces, and incoming and outgoing interfaces. It monitors the rate of pending interest with respect to overall traffic and when malicious traffic is detected their rate is limited. The number of malicious packets is also be reduced by limiting the size of the interface linking the attacker node at its access router [5].

A dual loop communication network with main and standby channels was introduced in [13] where the designed PI controllers were installed. Duration and frequency of DoS attacks are detected if the main channel exceeds the scheduled value obtained for stable conditions. Once the DoS is detected the communication channel is switched to a standby channel which acts as a backup to mitigate the impact of a serious DoS attack. However, this secondary channel might be targeted by a DoS attacker.

DoS mitigation via packet verification technique is proposed in [3] where packets are signed by the sender. Digital signatures are used to verify legitimate packets. If the MAC in a packet does not match with the one the forwarder generates from the received packet, then the packets are labeled as illegitimate and are dropped.

A cross-layered method that is applicable in all layers of the network model was proposed in [10]. A self-operating machine, Learning Automata (LA), was developed that responded to a sequence of instructions. DDoS in IoT devices are handled using three steps: DDoS detection, DDoS identification, and DDoS defense. Incoming traffics are analyzed in DDoS detection, and if the rate of incoming traffic exceeds the threshold DoS is detected and an alert, DDoS alert (DALERT), is sent. In DDoS identification, a list of all hosts sending requests is created to find the node/devices sending more number of packets. DDoS defense involves discarding packets from identified attackers.

To our best knowledge, no investigation of DDoS attack-defense model on a smart grid using co-simulation between the power and communication side has been proposed. We fill this gap by demonstrating how easy it is for an attacker to perform a DDoS attack in a smart grid and how a mitigation strategy could utilize token buckets to reduce the impact of a DDoS attack.

III. System Architecture

A. System Model

Photovoltaic (PV) is one of the major components in an electric grid. PV is a renewable energy source that converts solar radiation energy to electrical energy. Solar radiation is unpredictable and fluctuates with respect to time of day, environmental variables like weather, cloud, and the season. A battery energy storage system (BESS) can be used to smooth the fluctuation in the power generated from the PV. A BESS compensates during low production and high energy demand by providing stored energy. A controller is responsible for the communication between electric grid devices, including PV and BESS. The controller obtains measurements from one or more PVs and uses these to run optimization procedures to identify the setpoints for the BESS' in the grid for stability and resilience. In the real world, PV and BESS might not always be co-located. We have built a communication interface combining the power system and the communication network. This interface built on top of ns-3 is used to emulate devices on power grid communicating with each other. This provides a mechanism for near real-world assessment of the impact of the power grid performance given the stochastic nature of the communication network and the different attack vectors.

We used Optimal Reconfiguration and Resilient Control Framework for Real-Time Photovoltaic Dispatch to manage grid infrastructure (ReDis-PV) [1]. ReDis-PV is a control architecture that manages PVs and BESS' clusters based on a power grid dynamic model and a situation awareness model with the global controller resident at the control center or in the cloud. It is also responsible for hierarchical control with dynamic clustering, optimal power flow, and organization module. The dynamic clustering allows a group of DERs to form a cluster with the cluster represented by one of the DERs chosen as the *lead DER*. The lead DER of each cluster communicates with the global controller and receives setpoints from the global controller to deploy at each of the DERs in its cluster. This is how the generation at each PV is managed. As in this work, we are focused on the communication network part and the impact of DDoS attacks on the power grid applications.

In our previous work [8], we proposed a network architecture that provides differentiated service to application flows based on importance, latency, and reliability requirements into three classes. Protection related traffics are categorized as Type I traffic which requires low delivery latency and high delivery reliability. Control traffics were categorized as Type II as they require high reliability. Type III traffic class is reserved for other applications that did not impose stringent requirements and were categorized as best effort. To prioritize urgent flows and to rate limit non-urgent ones, we used a weighted fair queuing (WFQ) based scheduling of the packets at each router with three different queues, one for each traffic type/class [8]. Every incoming packet is assigned a weight based on its priority class.

To ensure that anyone particular flow does not commandeer the network the flows of all three types are rate-limited using a token bucket assigned to each flow type in each router. The token generation rate for each class is defined based on the priority of the class–higher priority traffic has a higher number of tokens generated per second compared to the tokens generated for the lower priority traffic. This enables the higher priority traffic to be able to receive favored access to the network compared to the lower priority traffic.

B. Threat Model

An electric grid system can be subject to attacks, like DoS and DDoS. DoS and DDoS attacks are common attacks that are easy to orchestrate and hard to prevent. DoS can be used to perform network jamming, network spoofing, and data flooding that delays or completely halts communication between DERs and other devices. This disruption in communication brings the devices out of synchronization. DDoS can mess up measurement gathering for the controller, and prevent setpoints from reaching BESS devices. This can affect grid stability and in the worst case lead to different types of grid failures. To study the extent of the impact on the system, we have modeled a realistic attack vector against controllers and DERs.

An adversary could be any node with intention of adversely affecting the network. Nodes in the electric grid can also be taken over and controlled by an adversary. An adversary can also take over multiple nodes of an electric grid, which can collude with each other to create a sophisticated distributed attack.

The lead DER transmits packets every second, and it is the one generating more packets compared to other DERs. It is very likely that if enough of the uniformly distributed attacker nodes collude, they could learn about the network topology and identify the lead DERs.

Node/attackers can collude with each other and keeps a log of packets they receive, and find the nodes transmitting the most number of packets. After analyzing the network for some time, attackers can create a list of the most active nodes. There is a high probability that these are lead DERs. An individual attacker can select a target from this list of possible lead DERs, and transmit a large number of packets to the target. The location of central controller, ReDis-PV is static and can be attacked too.

Algorithm 1 describes an attack model for attacker nodes to find the most popular node in the network. For about 50 seconds, attacker nodes check all the interest packets flowing through it and keep a log of nodes transmitting packets. Attackers then create a frequency log with popular nodes and the number of packets transmitted by that node. The 50s time window was chosen based on observed convergence of the popularity calculation. These attackers then collude and create a combined frequency log to find the most popular node throughout the network. Attackers select the top 12 nodes to attack. We choose 12 nodes for illustrative purposes; we arrived at this number by empirical observations. If the attackers attack the top 12 communicating nodes invariably all the lead

Algorithm 1: Attack Model

```
Result: Set Target For Attackers.
initialization;
for all attackers do
    while time ≤ 50 s do
        Use received interest packet to find DERs
         transmitting packets;
        Create a frequency log with nodes (DERs) and
         frequency count;
    end
    Create a combined frequency log with nodes
     (DERs) and frequency count;
    Select top 12 nodes (DERs) to attack;
    while time != End of Attack do
        Select the closest node (DER) from the list as
         target;
        Flood the target with 1000-1100 DoS attack
         packets per second;
    end
end
```

DERs are subject to a DDoS attack. In realistic settings the attackers can choose a certain number of popular nodes from the top of the ordered list. Each target node is attacked by two attackers generating 1000-1100 packets/second.

C. Mitigation Strategy

The DDoS attack is impossible to avoid, but its effect can be reduced by blocking traffic from questionable and non-legitimate sources. Algorithm 2 describes the steps we have used to mitigate the DDoS attack. We have implemented a DoS mitigation strategy that ensures packets are transferred, prioritizing Type I traffic over Type II and Type II traffic over Type III. These three types of traffic have three different queues. To forward a packet to an outgoing interface, it uses a token from the corresponding bucket. If the tokens run out, the packets will be de-queued from the queue.

The solution we developed leverages iCAAP's priority levels and introduces another class of priority, referred to as Type IV. Unlike the other priority classes, there is no defined name structure for Type IV packets; Type IV priority can only be set by an individual router and only on a local level. Type IV priority is defined as best effort. Like Type I, II, and III traffic, Type IV packets also have access to a token bucket where tokens are generated at a given rate. This allows us to remove potential DDoS flows from the base priority classes, freeing up those resources for legitimate traffic.

Each router maintains a nodal loss rate, which is updated whenever an interest is completes, whether it was satisfied, timed out, etc. Once the nodal loss rate passes a predefined threshold (system parameter), the router will begin to search for problematic packet prefixes. This is done by looking through a rolling history of received interests and choosing the most popular prefix and adding it to a list of prefixes that are monitored separately. Popular prefixes can be used

Algorithm 2: Mitigation Strategy

```
Result: Tag suspicious traffic to Type IV.
Packet Arrives;
if arrived packet prefix is monitored then
    if the loss rate is above Type IV threshold then
        Assign the packet Type to Type IV;
    else
        Set the packet Type denoted by name;
    end
end
if PIT Expires then
    if prefix is monitored then
        Update monitored entry loss for the interest;
    else
        Update nodal loss rate;
    end
    Update rolling history log for interests;
    if nodal loss exceeds nodal threshold then
        if Rolling history has history size entries then
            Check the rolling history for most popular
             prefix;
            Add interest to monitored list;
            Clear history;
            Reset loss rate;
        end
    end
end
if Interest is Satisfied then
    if interest prefix is monitored then
        Update monitored entry loss for interest;
    else
        Update nodal loss rate;
    end
    Update rolling history log for interests;
end
```

for determining attack packets. The nodal loss rate is then reset, and a loss rate is maintained separately for the monitored prefixes, which are now ignored by both the nodal loss rate and the rolling history. If these prefixes' loss rate surpasses a predefined loss threshold, it will henceforth be classified as a Type IV packet by the router, regardless of its previous priority class. During an attack, a router may repeat this process multiple times until the loss created by the DDoS attack flows no longer have a significant impact.

There is a chance for false positives in our detection system, in which case a legitimate prefix may be mistakenly classified as a Type IV packet. The prefix's monitored loss rate can fall under the Type IV threshold and have its original priority classification restored. Along with this, if a prefix can remain under this threshold for a predetermined amount of time the router will no longer monitor that prefix, removing its separate loss rate, and it will no longer be ignored by the nodal loss rate or rolling history. To ensure that a prefix will have a fair chance

of redemption, only packets that are forwarded from the router will affect the loss rate, and any packet that is dropped locally will not get added to the loss rate.

Algorithm 2 has a run-time complexity of $O(n)$, where n is the size of the rolling history we keep. All other operations are simple look-ups and thus do not add to the time complexity. The space complexity is $O(n)$, where n is the number of attacker prefixes, as potentially every attacker's prefix may be added to the list of monitored prefixes.

IV. Experiment & Results

A. Simulation setup

We created our communication network topology over IEEE-2500 bus topology. Simulation of an electric power distribution center was accomplished using OpenDSS, which supports distributed energy resources (DER) grid integration. The network portion of the simulation was carried out in the well-known discrete event network simulator, ns-3. The power system and communication system were both simulated in two different loosely coupled standalone devices. The co-simulation platform developed validated both the power system and communication system, enabling these domains with different time steps to be simulated together.

In the 2500-bus topology, we deployed 26 BESS' and 142 PV devices. A DDoS attack started in 20s and continued throughout the simulation. During the entire simulation, solar irradiance and load were between 0.8 and 1.0. Data generated were classified as Type I (data from controller to devices), Type II (data from the PVs and BESS' to the controller), Type III (other data), and Type IV (potentially malicious traffic) based on their priority. Type I traffics are high priority traffic and Type IV traffics have the least priority traffic. For Type I, II, III, and IV traffic token bucket fill rates of 600, 9500, 2000, and 100 respectively were selected and all of them had a capacity of 200 packets in their queues.

A list of the most popular devices was generated using algorithm 1. From that, a list the top 12 were selected as attack targets. These devices were then targeted by adversary nodes located on an average of 10-35 hops away. Four attackers were used to attack the controller, ReDis-PV. All the attackers generated packets at the rate of 1000-1100 packets/sec to flood the network. A payload of 7 Mb was added to the attack interests to intensify the effect of the attack. Our mitigation strategy used values of 0.6 & 0.8 for the nodal and Type IV thresholds respectively. These values were chosen so that the algorithm is more sensitive to the total nodal loss rate, as preferably that should be low. The Type IV loss rate is less sensitive, as the attackers send for non-existent packets, thus ensuring their loss rate should be 1.0.

B. Results

DDoS had a major impact on the loss and latency of packets as shown in Tables I, II, and III. In a normal run, loss rates for high-priority Type I and Type II traffic are zero. The DDoS attack throttles the network such that loss rates for all three types of traffic are increased. The mitigation strategy can greatly improve the success rate when under attack, bring the losses nearly down to zero. This is due to the use of the fourth traffic type (Type IV). By its implementation the architecture can handle most DDoS traffic; while providing access to the legitimate traffic.

TABLE I: Loss Rate (%)

	No DDoS	No Mitigation	With Mitigation
Type I	0.0	58.3	5.1
Type II	0.0	44.3	0.0
Type III	21.0	53.1	1.6

TABLE II: Latency (ms)

	No DDoS	No Mitigation	With Mitigation
Type I	17.8	4626.1	4197.0
Type II	13.7	3743.1	148.9
Type III	2025.1	1478.6	341.0

TABLE III: Setpoints and measurements loss (%)

	No DDoS	No Mitigation	With Mitigation
Setpoints	0.0	58.6	0.0
Measurements	0.0	42.1	0.0

Latency is greatly affected by the attack, as all the queues get filled up, leading to longer wait times for delivery. Mitigation can bring these latencies down, especially for Type II packets – going from 3.7 seconds to 150 ms. Breaking down the loss even further into the essential setpoint and measurement values, we see that without mitigation the losses are nearly 50% for both, and with mitigation- both are at zero. This implies that the communications for grid operations and stability will operate as needed in the event of a DDoS attack.

Netload is the view of the network state from the controller's perspective created from measurements. Power flow represents the true network state. On the power system side, the ability of the BESS devices to support the netload by changing the reference power was studied, along with the accuracy of the perceived netload from ReDis-PV's perspective. It takes about 60 seconds to set up and for ReDis-PV to have an overall view of the network. Figure 1 shows the netload of the system when BESS' are used. The netload in the event of a DDoS attack significantly diverges from that when there is no attack. With mitigation the netload is closer to that of the system when there is no DDoS attack–this demonstrates the efficacy of our framework. The time 46800 to 47300 represents the 500 seconds of simulation in terms of seconds of the day. Figure 2 shows the power flow graph. Power flow is the representation of the true power in the network. The results show that the DDoS attack without mitigation requires a lot more power than the one with mitigation. With

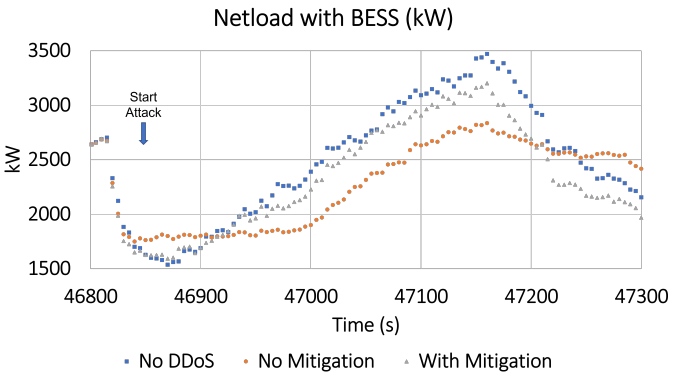

Fig. 1: Netload with BESS (kWh)

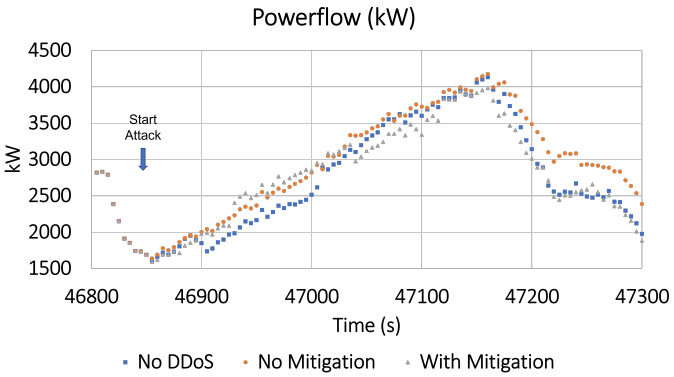

Fig. 2: Power Flow (kWh)

BESS, the controller dynamically changes the battery power to balance the changes in the PV power and netload. DDoS attack disrupts the flow of packets carrying setpoint and measurement information. As a result, power output from the BESS' are not aligned to the setpoint and measurement values.

The results demonstrate the efficacy of our framework in mitigating the DDoS attack's effects on the power network. It also shows that the network layer's deployment of the mitigation framework provides a much better way of meeting the QoS requirements while also helping prevent the impacts of DDoS attacks compared to the baseline approach.

V. Conclusion

In this paper, we presented the iCAD architecture for DDoS protection in smart grid systems. iCAD is an extension of our prior work iCAAP where traffic is classified into three categories (Type I, Type II, and Type III) based on their characteristics [8]. iCAD introduces a fourth traffic Type (Type IV) for suspicious traffic. Using co-simulation, we demonstrated that iCAD can successfully handle DDoS traffic and meet QoS expectations of applications. With the use of iCAD, Type I, II, and III loss rates were brought down to 5.1%, 0.0%, and 1.6% from 58.3%, 44.3%, and 53.1% respectively.

References

[1] Optimal Reconfiguration and Resilient Control Framework for Real-Time Photovoltaic Dispatch to Manage Critical Infrastructure (ReDis-PV). http://redispv.org/. [Accessed: September 2022].

[2] Calum Cameron, Charalampos Patsios, Phil C Taylor, and Zoya Pourmirza. Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes. *IEEE Transactions on Smart Grid*, 10(3):3010–3019, 2018.

[3] Xia Chen, Jianyu Zhou, Mengxuan Shi, Yin Chen, and Jinyu Wen. Distributed resilient control against denial of service attacks in dc microgrids with constant power load. *Renewable and Sustainable Energy Reviews*, 153:111792, 2022.

[4] Alberto Compagno, Mauro Conti, Paolo Gasti, and Gene Tsudik. Poseidon: Mitigating interest flooding ddos attacks in named data networking. In *38th annual IEEE conference on local computer networks*, pages 630–638. IEEE, 2013.

[5] Huichen Dai, Yi Wang, Jindou Fan, and Bin Liu. Mitigate ddos attacks in ndn by interest traceback. In *2013 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, pages 381–386. IEEE, 2013.

[6] David Freet and Rajeev Agrawal. An overview of architectural and security considerations for named data networking (ndn). In *Proceedings of the 8th International Conference on Management of Digital EcoSystems*, pages 52–57, 2016.

[7] Paolo Gasti, Gene Tsudik, Ersin Uzun, and Lixia Zhang. Dos and ddos in named data networking. In *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*, pages 1–7. IEEE, 2013.

[8] Anju K James, George Torres, Sharad Shrestha, Reza Tourani, and Satyajayant Misra. icaap: information-centric network architecture for application-specific prioritization in smart grid. In *2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5. IEEE, 2021.

[9] Shichao Liu, Xiaoping P Liu, and Abdulmotaleb El Saddik. Denial-of-service (dos) attacks on load frequency control in smart grids. In *2013 ieee pes innovative smart grid technologies conference (isgt)*, pages 1–6. IEEE, 2013.

[10] Sudip Misra, P Venkata Krishna, Harshit Agarwal, Antriksh Saxena, and Mohammad S Obaidat. A learning automata based solution for preventing distributed denial of service in internet of things. In *2011 international conference on internet of things and 4th international conference on cyber, physical and social computing*, pages 114–122. IEEE, 2011.

[11] Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications surveys & tutorials*, 13(2):245–257, 2010.

[12] Gelli Ravikumar, Dan Ameme, Satyajayant Misra, Sukumar Brahma, and Reza Tourani. icasm: An information-centric network architecture for wide area measurement systems. *IEEE Transactions on Smart Grid*, 11(4):3418–3427, 2020.

[13] Xing-Chen ShangGuan, Yong He, Chuan-Ke Zhang, Li Jin, Lin Jiang, Min Wu, and Joseph William Spencer. Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks. *Control Engineering Practice*, 107:104678, 2021.

[14] Won So, Ashok Narayanan, and David Oran. Named data networking on a router: Fast and dos-resistant forwarding with hash tables. In *Architectures for Networking and Communications Systems*, pages 215–225. IEEE, 2013.

[15] Reza Tourani, Satyajayant Misra, Travis Mick, Sukumar Brahma, Milan Biswal, and Dan Ameme. icens: An information-centric smart grid network architecture. In *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 417–422. IEEE, 2016.

[16] Ceeman Vellaithurai, Anurag Srivastava, Saman Zonouz, and Robin Berthier. Cpindex: Cyber-physical vulnerability assessment for power-grid infrastructures. *IEEE Transactions on Smart Grid*, 6(2):566–575, 2014.

[17] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang. Jamming sensor networks: attack and defense strategies. *IEEE network*, 20(3):41–47, 2006.

[18] Lixia Zhang, Alexander Afanasyev, Jeffrey Burke, Van Jacobson, KC Claffy, Patrick Crowley, Christos Papadopoulos, Lan Wang, and Beichuan Zhang. Named data networking. *ACM SIGCOMM Computer Communication Review*, 44(3):66–73, 2014.

[19] Xingsi Zhong, Iroshani Jayawardene, Ganesh Kumar Venayagamoorthy, and Richard Brooks. Denial of service attack on tie-line bias control in a power system with pv plant. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 1(5):375–390, 2017.