Cyber Security of Market-based Congestion Management Methods in Power Distribution Systems

Omniyah Gul M Khan, *Student Member, IEEE,* Ehab El-Saadany, *Fellow, IEEE,* Amr Youssef, *Senior Member, IEEE,* and Mostafa F. Shaaban, *Senior Member, IEEE*

***Abstract*—As the penetration rate of flexible loads and Distributed Energy Resources in the distribution networks increases, congestion management techniques that utilize Demand Side Management (DSM) have been developed. These are indirect methods that rely on information exchange between the Distribution Network Operator, aggregators, and consumers' meters to encourage customers to change their demand to relieve congestion. Cyber attacks against aggregators can compromise the operation of DSM-based congestion management methods, and hence, affect the security and reliability of electrical networks. In this paper, the vulnerability of indirect congestion management methods to Load Altering Attacks is studied. An optimization algorithm is developed to determine the aggregators a cyber attacker would compromise, via minimum alteration of their load profiles, to cause congestion problems. The impact of such attacks on congestion and consumers' electricity bill is then studied. A mitigation scheme is formulated to determine the most critical aggregators in the network. The security of these aggregators is then reinforced to mitigate such cyber attacks.**

***Index Terms*—Cyber security, Load Altering Attack (LAA), Congestion Management, optimization.**

I. Introduction

THE increased number of power-hungry flexible loads, such as Electric Vehicles (EVs) and Heat Pumps (HPs), has changed the operating conditions of the distribution system. Congestion, a condition caused as a result of the power flow exceeding a network asset's transfer capability, which was not of concern in the past, might now occur. This is due to the high power consumption of active loads and the weakening correlation between electricity prices and demand resulting from the increased penetration level of intermittent renewable resources. Such congestions result in voltage violations and/or thermal overloading, possibly damaging devices such as distribution transformers and feeders [1]. Thermal overloading of distribution transformers and feeders causes an increase of operating temperature affecting transformers aging (e.g., see IEEE C57.91-201 [2] and IEC 60076-7 [3]).

For the Distribution Network operator (DNO), congestion threatens its ability to provide reliable supply to the end users. Conventionally, to avoid congestion, network assets are reinforced, incurring a huge cost. To avoid or postpone such costs, the DNO would generally employ its cost-free methods, such as reconfiguration and reactive power control, to manage congestion in the network. If these methods did not succeed in eliminating the congestion, market methods using Demand Side Management (DSM) would be employed. DSM utilizes price-based or incentive-based methods to motivate consumers to shift their flexible consumption to off-peak time [4]. Price-based congestion management methods include Dynamic Tariff (DT) [5] and Distributed Dynamic Tariff (DDT) [4]. Incentive-based methods include subsidy-based methods [6] and conditional re-profiling products [7].

Market-based congestion management methods involve consumers, aggregators, and the DNO, as shown in Figure 1. Consumers are the owners of flexible and non-flexible loads and they hire aggregators to represent their needs in the electricity market. Aggregators are responsible for optimally scheduling their customers' flexible demand and representing them in the electricity market. The DNO is responsible for ensuring smooth power flow between suppliers and consumers and making sure that there is no congestion in the network.

All DSM-based congestion management methods rely on the communication between the DNO, aggregators, and consumers' meters in exchanging customers' preferences, price tariffs, and load schedules to relieve congestion [8], as illustrated in Figure 1. This reliance on the two-way flow of information between the different involved entities makes them prone to cyber attacks. Any theft or alteration of data could violate consumer privacy, cause economical damage, or even electrical outages. Hence, studying the vulnerability of indirect congestion management methods to cyber-attacks is vital.

The success of market-based congestion management methods relies on its cyber-security which needs to satisfy the *CIA* triad. The CIA triad symbolizes the Confidentiality, Integrity, and Availability of the cyber network which can pose significant threats to the grid if security vulnerabilities are not addressed. Confidentiality is needed to ensure authorized access to sensitive information, such as consumers' electricity demand. Integrity refers to the assurance that information, such as price signals sent to consumers meters, is authentic and not

O. Gul M Khan is with the Electrical and Computer Engineering Department, University of Waterloo, Waterloo, ON, Canada (e-mail: ogulmkhan@uwaterloo.ca).

E. El-Saadany is with the EECS Department at the Advanced Power and Energy Center in Khalifa University of Science and Technology, Abu Dhabi, UAE (e-mail: ehab.elsadaany@uwaterloo.ca).

A. Youssef is with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada (email: youssef@ciise.concordia.ca)

M. Shaaban is with the Electrical Engineering Department, American University of Sharjah, Sharjah, U.A.E (e-mail: mshaaban@aus.edu)

Manuscript received October 21, 2020; revised December 25, 2020 and February 04, 2021; accepted February 28, 2021.

 https://doi.org/10.1109/TII.2021.3065714

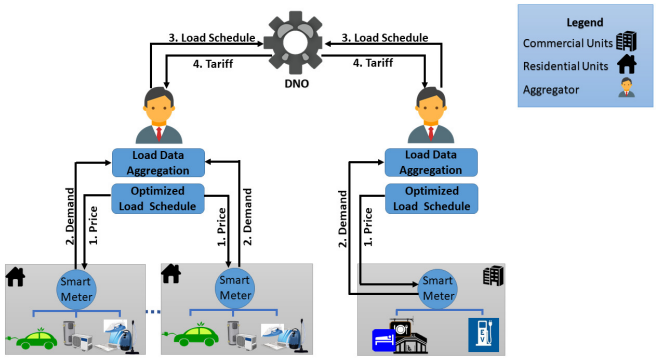

Fig. 1. Representation of DSM-based congestion management methods

corrupted. Finally, availability is the guarantee that authorized users have access to the required services at all times. For example, aggregators should be able to communicate their load demand readily with the network operator [9].

Attacks on consumers' meters and their communication links have been studied in the literature, a summary of which is illustrated in Table I. In [10] and [11], the impact of False Data Injection (FDI) attacks on price and load signals in a distribution system was studied. Denial of Service (DoS) and FDI attacks were adopted in [12] to compromise Home Energy Management Systems or its communication link with the DNO. Load Altering Attacks (LAA) were studied in [13] and [14]. Static LAA resulted in causing damage to network equipment as a result of circuit overflow [13] while closed-loop dynamic LAA had an impact on power system stability [14]. Load Redistribution Attacks (LRDA) were simulated in [15]. Different scenarios were simulated, representing various levels of network information possessed by an attacker.

Attacking the DNO is not easy since its control center is highly secure due to its significant role in the grid. Attacking aggregators or their communication link with the DNO is another aspect that can be utilized by a cyber attacker to affect congestion. The unique position of aggregators in the network, in terms of its connection to its DER equipment and the DNO, has been established in [16]. Hence, the importance of studying aggregators' cyber security as their actions, if attacked,

TABLE I
LITERATURE REVIEW OF CYBER SECURITY OF CONSUMERS METERS

Ref.	Attack	Compromises	Impact
[10]	FDI	Price signal and load data	1. Price attack causes change in demand resulting in price change. 2. Load attack results in wrong demand causing price change.
[11]	FDI	Price received by consumers	Change in demand causing instability, fluctuation in real-time pricing or voltage violations.
[12]	1. DoS 2. FDI	Price signal and load data	1. DoS causes load scheduling to temporarily become ineffective. 2. FDI results in random load schedules not reflecting market.
[13]	LAA	Internet connected loads	Circuit overflow causing damage to the utility and/or equipment.
[14]	Dynamic LAA	Vulnerable loads	Power system stability.
[15]	LRDA	Smart Meters	Circuit overflow causing damage to the utility and/or equipment

could have a considerable risk on the ecurity of the grid. A state-sponsored adversary can cause economic disruptions in the country as a result of hiding existing congestions which could result in load shedding. Attackers could also be hired by competitors to cause high tariffs to be imposed on the consumers due to unreal congestions encouraging them to change their utility provider. However, to date, the impact of cyber-attacking aggregators on market-based congestion management techniques has not been studied.

Motivated by the research gap, the effect of compromising aggregators and their communication link to the DNO on market-based congestion management techniques is studied in this paper. Load Altering Attacks (LAA) are modeled in the day-ahead market to modify cyber attacked aggregators' load profiles to cause or hide congestion in the distribution network. LAAs, which is a type of False Data Injection Attack (FDI), has been previously studied in the literature [14] - [13]. However, the impact of LAAs on the power system level was studied aiming to alter a certain volume of flexible loads in the network to cause frequency instability and circuit overflow in power systems. Hence, consumers smart meters and the DSM-signals received were altered. However, in this paper, the attack is assumed to target the day-ahead market making the network operator not capable of using bad-data detection techniques to detect the attack. The impact of such a cyber attack in terms of congestion and congestion tariffs is evaluated. To defend the electrical network against such cyber attacks, a mitigation scheme is then developed. Until recently, many studies have come up with mitigation schemes to defend against FDI attacks in the smart grid. In [17], a graphical approach was proposed to detect the most critical meters in the network and mitigate against FDI attacks. Optimization techniques were utilized in [18] and [19] to develop its optimal mitigation scheme determining the least number of sensor measurements that need to be protected. Game theory has also been used to study data injection attacks involving multiple adversaries [20]. A Stackelberg Game was used to model the strategic interactions between the defender and attackers aiming to identify the main network components that need to be secured. It should be noted that FDI attacks are dependent on an adversary's knowledge of the system. Hence, proactive methods attempting to change system characteristics, either via changing topology or impedance perturbation, have been developed in the literature. This adds an extra layer of protection against FDI. In [21], strategic switching of network topology has been proposed as a mechanism to mitigate FDI attacks. In [22], an algorithm is modeled to determine branches that need to be perturbed using Distributed Flexible AC Transmission System (D-FACTS) devices to minimize the possibility of stealthy FDI attacks. Feasibility and limitations of proactive FDI detection scheme through branch impedance perturbation was studied in [23]. However, existing literature have not determined the critical aggregators in the distribution network that needs to be secured against cyber attacks. In this paper, Mixed Integer Non-Linear Programming (MINLP) is used to model the mitigation scheme for single- and multiple-point load altering attacks. The optimization problem is solved using the Generalized Benders Decomposition (GBD) ap-

proach to determine the critical aggregators in the network. These aggregators are secured by the network operator to make the grid more resilient to such cyber attacks.

The main contribution of this paper is, hence, to identify cyber vulnerabilities of DSM-based congestion management methods as a result of a LAA on aggregators and to develop a mitigation scheme against such attacks. This contribution is achieved by fulfilling the following objectives:

- Distributed and centralized market-based congestion management techniques are studied. Vulnerability of Distributed Dynamic Tariff (DDT) congestion management methods to cyber attacks is then assessed.
- Develop an attack model that achieves various adversary objectives in compromising aggregators. The attack model is formulated from the attacker's perspective minimizing the number of aggregators needed to be compromised in the network.
- Develop a mitigation scheme to determine the critical aggregators in the network to secure. The mitigation scheme is prepared from the network operator's perspective, assuming the worst case scenario, to secure the aggregators in the network which if compromised would result in a stealthy attack. The problem is formulated as a MINLP and is solved using a decomposition technique.
- Verify the effectiveness of the proposed models by simulating the IEEE 33 bus network to evaluate a cyber attack's impact on congestion and congestion tariffs.

The remainder of the paper is organized as follows: Section II introduces the DDT congestion management method and the formulation of the LAA model. The IEEE 33 bus system is illustrated as a case study in section III to demonstrate the effect of attacks on the network. In section IV, a mitigation scheme is proposed to determine the critical aggregators that need to be secured in the network, followed by the conclusions.

II. Modeling of a Load Altering Cyber Attack

To study the vulnerability of congestion management methods to cyber attacks, the Distributed Dynamic Tariff (DDT) technique, proposed in [4], is initially simulated. The DDT method is adopted in this paper due to its distributed nature compared to the centralized dynamic tariff method [24] in which the network operator is responsible for forecasting the electricity prices and the flexible load in the network. However, if the DNO's forecast is inaccurate, then the congestion tariff imposed would not be an effective solution for congestion mitigation. On the other hand, in the DDT method, aggregators are responsible for providing their load forecast to the network operator, and hence, the DNO is not solely responsible for determining the congestion tariff. This distributed calculation of the congestion tariff increases the certainty and transparency of the model. In this section, the DDT technique is briefly explained before describing the attack model adopted. LAA are then modeled to determine the aggregators that require minimum scaling of their load portfolio to compromise to achieve the objective of the cyber attacker.

A. Distributed Dynamic Tariff (DDT)

In the DDT method [4], aggregators utilize quadratic optimization to determine their customers' optimal load schedule. This load schedule should meet the consumers preferences while minimizing their consumption cost. Hence, the resulting aggregators' optimal schedules can be represented as,

$$P^a_{i,t} = E(P^{a,nf}_{c,t} + P^{a,f}_{c,t}), \forall a \in N_a, \forall i \in N_d, \quad \forall c \in N_m, \forall t \in N_T \tag{1}$$

where $P^a_{i,t} \in \mathbb{R}^{N_d}$ is the load of bus i of aggregator a at time t. N_a, N_d and N_m are the set of aggregators, buses, and customers in the distribution network. N_T is the total set of time slots considered in the day-ahead market. E is the customer-to-bus mapping matrix where $E \in \mathbb{R}^{N_d \times N_m}$. $P^{a,nf}_{c,t}$ and $P^{a,f}_{c,t}$ are the non-flexible and flexible loads of customer, c, of aggregator a at time t, where $\{P^{a,nf}_{c,t}, P^{a,f}_{c,t}\} \in \mathbb{R}^{N_m}$.

The optimal load schedule of the aggregators, $P^a_{i,t}$, are forwarded to the DNO who is responsible for determining the resulting congestion tariff, referred to as Distributed Dynamic Tariff (DDT). The DNO determines the total complex power, $S_{i,t}$, for each bus using both the flexible and non-flexible load demands of the consumers. DC load flow analysis [4] is then used to determine the voltage level of each bus and the power flow in each line. The results obtained are compared with the network limits to determine the extent to which the branch thermal limit and the node voltage limits have been violated. Capacity violation of a branch is represented using marginal price λ_t, while the violation of voltage limits is represented using marginal price w_t. Consequently, congestion tariff, r_t, is determined for each bus as shown in (2)-(4).

$$\lambda^{(k+1)}_{i,j,t} = \lambda^{(k)}_{i,j,t} + \alpha(F_{i,j,t} - F^{max}_{i,j}), \forall t \in N_T \tag{2}$$

$$w^{(k+1)}_{i,t} = w^{(k)}_{i,t} + \alpha(-1 + \frac{1}{V_0^2} Re(Z\overline{s^{(k)}_t}) + \frac{\underline{V}}{V_0}, \forall t \in N_T \tag{3}$$

$$r^{(k+1)}_{i,t} = D^T \lambda^{(k+1)}_{i,j,t} + \frac{Re(Z^T)}{V_0^2} w^{(k+1)}_{i,t}, \forall t \in N_T \tag{4}$$

where k is the iteration number, $\lambda^{(k+1)}_{i,j,t}$ is the updated marginal price based on how much the power, $F_{i,j,t}$, flowing at time, t, has exceeded the branch (i,j) maximum power flow limit, $F^{max}_{i,j}$. $w^{(k+1)}_{i,t}$ is the updated marginal price, $\underline{V}$ is the lower voltage limit, V_0 is the voltage at node 0, α represents the step size, Z is the partial nodal impedance matrix, and D represents the bus to branch mapping matrix. Since the DDT method imposes tariffs to decrease demand at congestion times, the marginal prices are required to be non-negative. This iteration continues between the DNO and the aggregators, who would re-optimize their load schedule and communicate it back to the DNO, until $\mid r^{(k+1)}_{i,t} - r^{(k)}_{i,t} \mid$ converges to a small value.

B. Attack Model

For the DNO to determine the congestion tariff, consumers need to submit their flexible load utilization preferences to their respective aggregators. In turn, the aggregators need to submit their day-ahead load schedules to the DNO. Hence, the

communication network of the smart grid forms the basis of information exchange between the consumers' smart meters, the aggregators, and the network operator. As illustrated in Figure 1, Home Area Networks (HAN) are deployed at the lowest level, within residential and commercial units, to connect the various flexible and non-flexible loads of the consumers to the smart meters. The Neighborhood Area Network (NAN) is utilized to connect the aggregators to their customers' smart meters. And finally, Wide Area Networks (WANs) are utilized to facilitate communication between the aggregators and the utility operator. Aggregators, hence, can communicate their optimal load schedules to the DNO, which in turn, computes and conveys the congestion tariff to them. Congestion management methods' cyber reliance on the DNO's control center, the aggregators' management systems, the consumers' smart meters, and the communication infrastructure makes these points vulnerable to a cyber attack if not secured properly.

In this paper, the vulnerability of indirect congestion management methods to cyber attacking aggregators or their communication link with the DNO, affecting the integrity of aggregators load profiles is studied. The attack model involves the following assumptions:

- The attacker has knowledge of subnetwork, $\mathbb{S}$, of the distribution system's topology [25] [26].
- The attacker is assumed to have been eavesdropping on $\mathbb{S}$ and hence, has knowledge of its historical load data [25].
- The attacker is capable of performing load flow analysis to predict which aggregator to attack [27] [25].
- All aggregators are assumed to have no incentive to lie.
- All aggregators are equally prone to be attacked.

The main objectives of the attacker for compromising aggregators can be summarized as follows:

- Create fake congestions causing the distribution network operator to impose high congestion tariffs.
- Alter aggregators' response to a congestion tariff imposed resulting in fake congestion.
- Hide congestion from being detected in the day-ahead market causing unresolved congestion in real-time.

Based on the aforementioned attack assumptions and objectives, the following section explains the modeling of load altering attacks compromising aggregators in the network.

C. Load Altering Attacks (LAA)

To determine possible congestions and calculate the congestion tariff, the DNO relies on the load profiles, $P^a_{i,t}$ (1), received from the aggregators in the network. In a LAA, an attacker compromises N_c aggregators of the existing N_a aggregators and changes their load profiles, $P^a_{i,t}$, that is sent to the DNO. The attacker is assumed to have been eavesdropping on $\mathbb{S}$ and has collected enough historical data to determine when a specific feeder is near congestion. The attacker then formulates an optimal attack to minimize the number of aggregators, N_c, needed to be compromised by solving the following mixed integer non-linear problem (MINLP):

$$\min \sum_{a \in N_a} A^a \tag{5}$$

A^a is a binary variable equal to 1 if aggregator a or it's link with the DNO is attacked and 0 otherwise. Moreover, assuming a worst-case scenario in which an attacker has knowledge of $\mathbb{S}$ and historical load forecast (e.g. a disgruntled employee at the utility who has access to such information), the attacker uses equality constraint (6) to perform power flow analysis and compute the power flowing in each branch.

$$\begin{aligned} P^G_{i,a} - P^L_{i,a}(1+\Delta^a_i) &= V_i \sum_{j}^{N_{bus}} V_j(G_{ij}\cos\delta_{ij} + B_{ij}\sin\delta_{ij}) \\ Q^G_{i,a} - Q^L_{i,a}(1+\Delta^a_i) &= V_i \sum_{j}^{N_{bus}} V_j(G_{ij}\sin\delta_{ij} - B_{ij}\cos\delta_{ij}) \end{aligned} \tag{6}$$

where $\{P^G_{i,a}, Q^G_{i,a}\}$ are the generated real and reactive power at bus i of aggregator a, $\{P^L_{i,a}, Q^L_{i,a}\}$ are the load real and reactive power, Δ^a_i is the change in aggregator's a bus i load demand due to a cyber attack, V_i is the voltage at bus i, $\{G_{ij}, B_{ij}\}$ are the conductance and susceptance of the (i,j) element of the admittance matrix, and δ_{ij} is the difference between voltage angles of bus i and j. Moreover, equality constraint (7) is used to optimally attack the load profiles of the buses as follows,

$$\Delta^a_i = A^a X^a_i, \forall i \in N_d, \forall a \in N_a \tag{7}$$

where X^a_i is the attack value for bus i. Since DSM-based congestion management is performed day-ahead, the network operator cannot use bad data detection and compare the power flows with a real-time estimate or measurement to know if it's false data or not. Instead, to make sure that it does not raise any alarms, constraints (8) and (9) are used as follows,

$$-\gamma \leq X^a_i \leq \gamma, \forall i \in N_d, \forall a \in N_a \tag{8}$$

$$0.95 \leq V_i \leq 1.05, i \in N_d \tag{9}$$

where γ is the maximum scaling factor of the compromised aggregators' load schedule. LAA causes congestion to increase or decrease compared to reality based on the objective of the attacker to increase or hide existing congestion. The formulation of these two attack models is explained next.

1) Creating and/or Increasing Congestion

To cause and/or increase congestion in a feeder connecting buses x and y in the distribution network, constraint (10) is imposed to ensure that the power flowing in branch (x,y) is larger than its maximum power flow limit $P^{max}_{i,j}$.

$$P_{i,j} > P^{max}_{i,j}, \text{for } i = x \text{ and } j = y \tag{10}$$

Moreover, the lower limit of constraint (8) is set to zero to have only positive scaling factors, X^a_i. This ensures that the attack is increasing the existing load profile, $P^a_{i,t}$, of the compromised aggregator causing or creating congestion in branch (x,y).

Hence, MINLP (11) needs to be solved using peak time data to obtain the minimum number of N_c aggregators to compromise and their respective attack vectors, X^a_i, for different maximum scaling factors, γ.

$$\begin{aligned} &\min \sum_{a \in \mathbb{A}} A^a \\ &\text{s.t. } (6) - (10) \end{aligned} \tag{11}$$

The binary variable, A^a and the power flow constraints, causes the non-convexity of (11). Hence, the results obtained can represent a local optimal solution. However, a local optimal solution is sufficient to achieve the objective of the attacker to create a fake congestion impacting congestion tariffs. The attacker hence compromises the resulting aggregators, N_c, and scales their load profiles, $P^t_{i,a}$, using their corresponding attack values obtained by solving (11). These load profiles are then received by the DNO who then attempts to relieve the increase in congestion seen as a result of the cyber attack by imposing larger congestion tariffs, $r_{i,t}$.

2) Hiding Congestion

An attacker is also capable of compromising aggregators' load profiles such that congestion is masked. This would result in the DNO not to take any corrective actions to resolve existing congestion. No tariff is imposed to decrease demand at peak times. Eventually, congestion needs to be dealt with in real-time otherwise the network assets would be affected. To perform such an attack, the attacker uses historical data obtained from eavesdropping to determine the typical time in which congestion is seen. The attacker determines the optimal minimum number of aggregators to attack, N_c, solving the following,

$$\min \sum_{a \in \mathbb{A}} A^a \tag{12}$$

$$\text{s.t.} (6) - (7), \text{ and } (9) \tag{12a}$$

$$P^{max}_{i,j} - \beta < P_{i,j} < P^{max}_{i,j} \tag{12b}$$

$$-\gamma \leq X^a_i \leq 0, \forall i \in N_d, \forall a \in N_a \tag{12c}$$

Inequality constraint (12b) has been added to obtain the attack values for the compromised buses such that the power flowing in the feeder of interest is less than its maximum limit ensuring that congestion is not detected by the congestion management program. However, to avoid the optimization algorithm setting the power flowing in the main branch to zero, parameter β is added as a very small number to ensure the stealthiness of the attack. Moreover, the attack value, X^a_i is limited to negative values to decrease the compromised aggregators' load profiles using (12c).

Solving MINLP (12), the resulting attack vectors, X^a_i, are used to modify the load profiles of the N_c aggregators. Being a non-convex problem, the results can represent a local optimum solution. However, a locally optimal solution suffices to achieve the objective of the attacker to hide existing congestion affecting the effectiveness of the technique in relieving congestion in the day-ahead market.

Figure 2 summarizes the process involved in calculating congestion tariff. It also demonstrates the parallel work of the attacker in compromising aggregators' load profiles to achieve its objective of faking or hiding congestion.

III. Case Study

To simulate the DDT congestion management method, the IEEE 33 bus system [28], illustrated in Figure 3, is utilized. Having 32 load buses, the IEEE 33 bus system is represented by nine aggregators having comparable loads. All the load buses, except bus 23 and 24, are assumed to be residential,

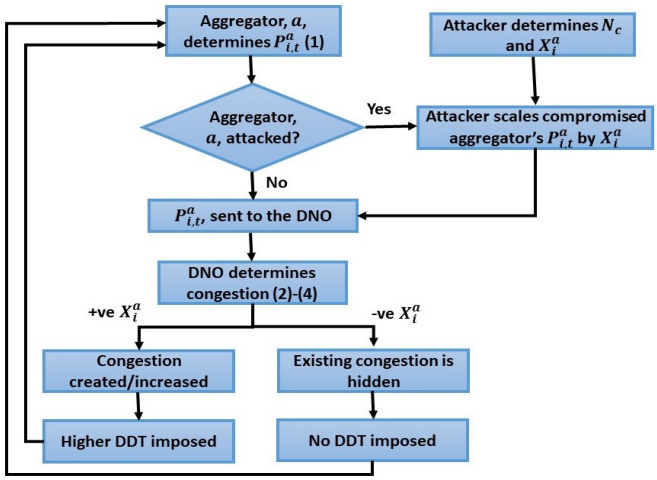

Fig. 2. Flowchart of cyber attack on DDT-congestion management method

having both flexible and non-flexible loads. Residential base load profiles are designed to have a maximum load equivalent to the default loading of the IEEE 33 test bus system. Table II represents the base load of the residential buses of the IEEE 33 bus system and the number of houses per bus. On the other hand, residential flexible loads are represented by one EV and one HP per house. Having the largest base load, load bus 23 and 24 were utilized as commercial buses consisting of Fast Charging Direct Current (FCDC) EV charging parking lots. These buses are represented by aggregators 6 and 7 respectively. Table III illustrates the various parameters needed for simulating the operation of the HPs and EVs. Data obtained from Toronto Parking Authority (TPA) [29] representing the daily hourly arrival and departure times of combustion engine cars in a commercial area parking lot in Toronto was used to simulate the availability of EVs in the commercial lots. In the absence of an EV from the lot, the EV was assumed to be at home. A subset of the TPA data was utilized such that the minimum parking duration exceeds the charging time required. The initial state of charge (SOC) of each EV is randomized to be uniformly distributed between 20% and 30% and is assumed that the EV needs to be completely charged on departure. Day-ahead electricity prices are obtained from the PJM market. GAMS [30] was used for executing the optimizations, and MATLAB was used for determining the congestion tariff imposed by the DNO to relieve congestion.

A. Choice of maximum scaling factor, γ

Scaling factor, γ (8), was used to limit the maximum change in the load portfolio, $P^a_{i,t}$, of the compromised aggregators.

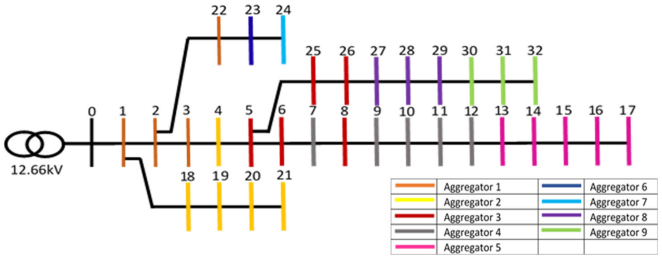

Fig. 3. IEEE 33 bus system load buses divided among nine aggregators [28]

TABLE II
RESIDENTIAL BUS LOADING

Bus #	No. of Houses	Load (kW)	Bus #	No. of Houses	Load (kW)	Bus #	No. of Houses	Load (kW)
2	25	100	12	16	60	22	23	90
3	23	90	13	16	60	25	22	90
4	31	120	14	29	120	26	15	60
5	16	60	15	15	60	27	15	60
6	15	60	16	15	60	28	15	60
7	50	200	17	15	60	29	30	120
8	51	200	18	23	90	30	50	200
9	15	60	19	23	90	31	38	150
10	15	60	20	23	90	32	53	210
11	12	45	21	23	90	33	16	60

TABLE III
CASE STUDY PARAMETERS

Variable	Value	Variable	Value
COP	2.2	Residential Areas	1500-2500 sq.ft
Residential Height	8.2 ft.	Temperature Range	18-24°C
EV battery size	36 kWh	Residential EV power	11 kW
FCDC EV power	50 kW	Initial SOC of EV	0.2-0.3
Power flow limit	7.91 MW	Voltage limits	0.95-1.05 pu

Simulations were carried out in MATLAB R2018a using a PC with an Intel Core(TM) i7-4790 CPU, 3.6 GHz, and 8 GB RAM to study the effect of γ on the convergence time of the DDT congestion management method. As illustrated in Table IV, $\gamma = 0$ represents a system that is not compromised. Time needed to determine congestion tariff was observed to increase from 286 seconds, for $\gamma = 0$, by 168% for $\gamma = 1$, and by 573.6% for $\gamma = 2$. This increase is as a result of requiring more iterations to shift the flexible demand of consumers to other times while meeting their preferences. However, the attacker only needed to compromise one aggregator to achieve its objective. Larger values of scaling factors, ($\gamma > 1$), would result in larger attack values that would increase the chances of being detected by the DNO. A scaling factor, γ, less than 0.05 was observed to not cause congestion while a γ larger than 2 was observed to cause non-convergence of the congestion management optimization problem. This results in the congestion not being relieved from the network. To avoid risking the stealthiness of LAA, the attack implemented should not cause the loads to largely deviate from their original values as it will raise alarms. Hence, γ of 0.1 and 2 were chosen to study the impact of a stealthy attack versus an extreme attack on congestion in the network.

B. Creating and/or Increasing Congestion

Using historical data, the attacker is aware that the main branch is near congestion at peak time. Utilizing peak time data, (11) is solved, for $\gamma = 0.1$, to obtain the minimum number of aggregators, N_c, to compromise and their respective attack vectors, X_i^a. Aggregators 3, 6, and 7 were identified as optimal aggregators to be compromised with maximum attack values, X_i^a, of 0.0683, 0.0856, and 0.0964 respectively. However, on changing γ to 2, (11) resulted in compromising only aggregator 7 with an attack value of 1.9981. These attack values are then utilized to alter the load profiles of the aggregators by Δ_i^a (7) before being sent to the DNO to determine the congestion tariff using (2)-(4).

TABLE IV
EFFECT OF γ ON CONVERGENCE TIME

γ	Convergence time (sec)	% Increase in time	No. of compromised aggregators
0	285.843877	-	-
0.1	422.279258	47.73%	3
0.5	509.393095	78.21%	1
1	766.977701	168.32%	1
2	1925.429139	573.6%	1

Figure 4 depicts the effect of the LAA on the power flow in branch $(0-1)$ of the IEEE 33 bus system. As observed, in the absence of an attack, the power flow in the main feeder is already congested at time 12 as it is peak time and demand for FCDC charging is high. For $\gamma = 0.1$, the optimal attack values, X_i^a, determined from solving (11), increases the aggregators load profiles. Consequently, the power flow in branch $(0-1)$ increases, and the impact of the attack is significantly observed between times 10 to 12 since the commercial bus is most active at that time. As observed in Figure 4, congestion at $t = 12$ is observed to increase, and a fake congestion is created at $t = 10$ and 11 though the main feeder, in reality, is not congested. This fake congestion would then be attempted to be redistributed to other times using the congestion tariff imposed. The aggregators would attempt to encourage the consumers to shift their demand to other times. However, when $\gamma = 2$, altering the load profile of aggregator 7 by 1.9981 (the attack value obtained solving (11)), resulted in a fake increase in congestion at times 9 to 12. This unreal congestion has to be dealt with by the DNO in the day-ahead market. Moreover, at $t = 12$, the existing congestion increased drastically causing the network operator to impose a much higher tariff if the attack goes undetected. However, since the DNO would have historical data and would perform short term load forecast, the chances of such an attack being detected are high.

Figure 5 demonstrates the effect of the LAA on congestion tariff, $r_{i,t}$, imposed by the DNO. In the absence of an attack, the imposed tariff increases the price of electricity at $t = 12$ by 16.6% to clear the congestion. Also, no tariff was imposed at $t = 10$ and 11 since there was no congestion. However, a LAA results in a higher DDT at congestion times to alleviate the increased levels of feeder overload. A LAA, with $\gamma = 0.2$,

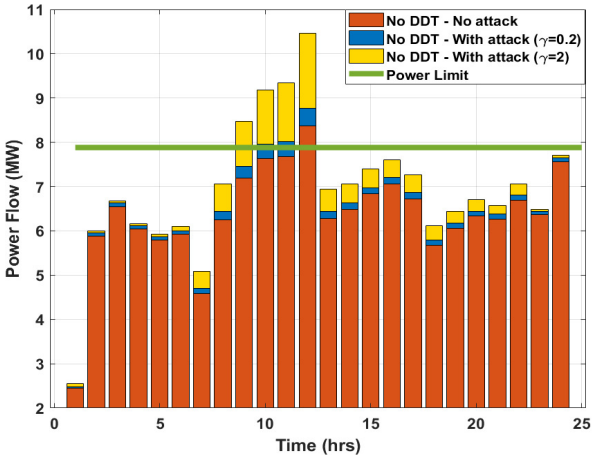

Fig. 4. Impact of a LAA on the loading of line 0-1

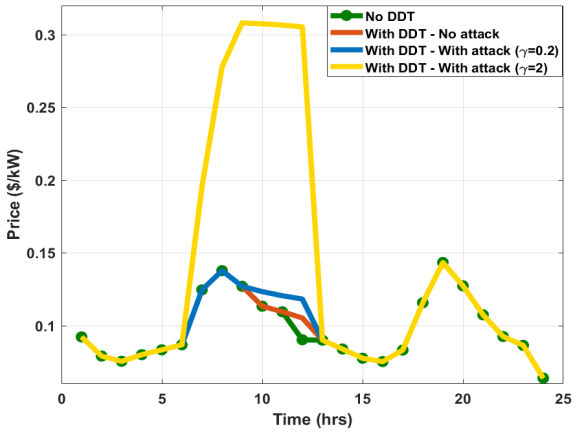

Fig. 5. Impact of a positive attack value LAA on the electricity price

increases the imposed tariff by an unnecessary 14.4% at $t = 12$. Customers, hence, have to pay a higher DDT of $0.028\$/kW$ instead of $0.015\$/kW$. Also, as a result of the unreal congestion being created at $t = 10$ and 11, a needless tariff is imposed by the DNO to solve the fake congestion. Customers who cannot change their demand from those times now have to pay 8.82% and 10% more at $t = 10$ and 11 respectively. This corresponds to approximately an increase of $0.01\$/kW$. Customers are, otherwise, inconvenienced in changing their demands to other times which in reality is unnecessary. On the other hand, for a LAA with a $\gamma = 2$, the imposed DDT at $t = 12$, increases the price by a needless 237%. Customers, hence, have to pay a higher DDT of $0.3053\$/kW$ instead of $0.1063\$/kW$. Also, as a result of fake congestion being created at $t = 10$ and 11, an unnecessary tariff is imposed by the network operator. Customers now have to pay approximately 170% more at $t = 10$ and 11, which corresponds to an increase of approximately $0.195\$/kW$. Moreover, at $t = 9$, customers should now pay 142% more for their demand which corresponds to an increase of $0.181\$/kW$.

C. Hiding Congestion

Using historical data, the attacker is assumed to be aware that the main branch is congested at peak time corresponding to $t = 12$. Hence, using peak time data, MINLP (12) is solved to obtain the minimum number of aggregators to compromise and their respective attack vectors, X_i^a. Note that in this case scenario, negative γ values are adopted to ensure that the compromised aggregators' load is lower than reality causing congestion to be masked. In our simulation, $\gamma = 0.1$ is chosen to avoid large differences from the original load profile and not raise any alarms, ensuring the stealthiness of the attack.

Solving (12) for $\gamma = 0.1$ results in identifying aggregators 3, 6, 7, and 9 that an attacker should compromise to hide congestion. The maximum attack values, X_i^a, for the four aggregators were determined as -0.0876, -0.0983, -0.0999, and -0.0820 for aggregators 3, 6, 7, and 9 respectively. These attack values are then utilized by the attacker to compromise the aggregators' load profiles by Δ_i^a (7) for $a = 3, 6, 7$, and 9 to mask the existing congestion. All aggregators in the network send their load profiles to the DNO who determines the congestion tariff using (2)-(4). However, as a consequence of the attack which decreased the compromised aggregators load profiles, congestion of branch $(0 - 1)$ of the IEEE 33 bus system at $t = 12$ was successfully masked. The network operator, seeing no congestion, does not impose any tariff. In reality, a DDT of 16.6% of the electricity price should have been imposed by the DNO to relieve the congestion that was masked. Moreover, branch $0 - 1$ was near congestion at $t = 10 - 11$. But, as a result of the LAA, the line is observed to be less congested than reality. This will cause a problem in real-time as customers have not been motivated to shift their demand to off-peak times. The DNO has to then try to solve the congestion otherwise network assets will get affected.

D. Computational Scalability

To test the effect of LAA on congestion management in terms of scalability, the IEEE 70 bus system [31] was simulated. The IEEE 70 bus system is an 11-kV radial distribution system having 70 nodes and 79 branches. Similar to the case study adopted, the system is represented using nine aggregators responsible for comparable loads. All the load buses except bus 57 are assumed to be residential, having both flexible and non-flexible loads. Residential non-flexible base load profiles are designed to have a maximum load equivalent to the IEEE 70 bus system default loading. Residential flexible loads are represented by one EV and one HP per house. Having the largest base load, bus 57 is utilized as a commercial bus consisting of FCDC EV charging parking lot with a maximum capacity of 150 EVs. Table V illustrates the scalability study of an attacker determining the optimal aggregators to attack in the IEEE 70 bus system versus that of the 33 bus system. The case studies were implemented on a PC with an Intel Core(TM) i7-4790 CPU, 3.6 GHz, and 8 GB RAM. As the number of variables and constraints needed to be solved increased, the time required by the attacker to determine the critical aggregators in the network increased. However, since this computation is executed offline in the day-ahead market, this increase in time would not cause a problem to the attacker.

E. Discussion

Congestion management techniques dependence on the communication infrastructure makes them vulnerable to cyber attacks. A LAA can create or hide congestion. In the event of a cyber attack compromising aggregators causing fake congestion, congestion tariffs are imposed on consumers increasing their expenditure on purchasing electricity. If the cyber attack continues without it being detected, consumers would be motivated to change their aggregator representative to decrease their cost. On the other hand, a LAA that results in not managing congestion in the day-ahead market, would force the DNO to use active power control in the real-time

TABLE V
COMPUTATIONAL SCALABILITY OF LAA

Description	IEEE 33	IEEE 70
No. of variables in (11)	4647	19623
No. of constraints in (11)	4582	19486
Execution time to determine aggregators to attack	2.936 sec	4.581 sec

market. This results in shedding unnecessary loads to prevent activation of protection devices, following National Electric Code article 240 [32]. Load is disconnected from overloaded buses at times when electricity demand is maximum, resulting in dissatisfied customers [33]. Other attacks, such as denial-of-service attacks and load replay attacks can compromise the performance of such congestion management techniques. However, due to limited space, vulnerability of congestion management methods was demonstrated using only LAA.

IV. LAA Mitigation Scheme

In the previous sections, load altering attacks impacting congestion management methods was introduced, modeled, and simulated. In this section, a mitigation scheme, executed by the DNO, is proposed to determine the impact that different adversaries with varying intrusion capabilities can have on congestion. An attack that can compromise only one aggregator would require a higher attack value to achieve its objective risking the stealthiness of the attack. However, to compromise multiple aggregators using low attack values, strong cyber intrusion capabilities, as well as a larger effort, is needed to avoid being detected. The LAA mitigation scheme proposed identifies the critical aggregators in the network that would be the first choice for an adversary to attack. The term "critical aggregator" refers to aggregators that can be compromised using minimal attack values to achieve the objective of a cyber attacker while evading detection. A mixed-integer nonlinear problem (MINLP) is proposed to determine the attack-prone aggregators in the network. Generalized Benders Decomposition (GBD) algorithm is then utilized to solve the problem. The DNO would then increase the security enforcement of the resulting critical aggregators and their communication links preventing them from being compromised.

A. Optimization Problem Formulation

MINLP is used to determine the critical aggregators that would be the first point of attack by an adversary aiming to minimize attack values. Besides the constraints considered in (11), equality constraint (13) is enforced to ensure that the total number of compromised aggregators is equal to N_c.

$$\sum_{a \in N_a} A^a = N_c \tag{13}$$

Hence, to determine the critical aggregators which would be the first point of attack by an attacker that aims to create and/or increase congestion, the following MINLP needs to be solved:

$$\begin{aligned} &\min \sum_{a \in N_a} \sum_{i \in N_d} X_i^a \\ &\text{s.t. } P_{i,j} > P_{i,j}^{max}, \text{for } i = x \text{ and } j = y \\ &\text{and } (6) - (9) \text{ and } (13) \end{aligned} \tag{14}$$

where the lower limit of γ (8) is set to 0 to ensure the increase in the load of the compromised aggregator. On the other hand, to hide existing congestion, MINLP (14) is solved with the upper limit of γ (8) set to 0. This is done to ensure the decrease in the profile, $P_{i,t}^a$, of the compromised aggregator. Moreover, the power flow inequality constraint is changed to ensure that the power flow in the branch being attacked is lesser than its maximum limit, $P_{i,j}^{max}$. Figure 6 summarizes MINLP (14) used to determine the critical aggregators in the network and their corresponding attack values.

MINLP (14) is a non-linear and non-convex problem due to: (i) non-linearity of equality constraint (7), (ii) non-linearity and non-convexity of power flow equations (6), and (iii) non-convexity caused by the binary variable, A^a. This causes the determination of a global solution for the optimization problem difficult. These problems were tackled to succeed in obtaining a global solution for the mitigation scheme proposed.

B. Linearization of the product of two variables

The equality constraint (7) is nonlinear due to it being the product of a binary variable, A^a, and a continuous bounded variable, X_i^a. To linearize (7), the following constraints were added to our MINLP formulation [34],

$$X_i^a - (1 - A^a)\overline{X_i^a} \leq \Delta_i^a \leq X_i^a - (1 - A^a)\underline{X_i^a} \tag{15}$$

$$A^a \underline{X_i^a} \leq \Delta_i^a \leq A^a \overline{X_i^a} \tag{16}$$

where $\overline{X_i^a}$ and $\underline{X_i^a}$ represents the upper and lower limits of the attack value, X_i^a. Hence, if the binary variable $A^a = 1$, then equation (15) makes $\Delta_i^a = X_i^a$, and (16) enforces that Δ_i^a is bounded within its limits. However, if the binary variable $A^a = 0$, then equation (16) makes $\Delta_i^a = 0$, and (15) enforces the limits on X_i^a. Thus, $\Delta_i^a = X_i^a A^a$. It should be noted that, given γ is a constant, for mitigating an attack that aims to create congestion, $\overline{X_i^a}$ represents γ while $\underline{X_i^a} = 0$. On the other hand, for mitigating an attack that aims to hide an existing congestion, $\overline{X_i^a} = 0$, while $\underline{X_i^a}$ represents negative γ.

C. Power Flow Equations Relaxation

Researchers have proposed numerous relaxation and approximation methods to convexify power flow equations. Convex relaxations increase the feasible space to include the non-convex feasible space, providing a lower bound solution to the non-convex problem (for a minimization) [35]. Moreover, convex relaxations can be exact for certain optimization problems making their solution globally optimal. However, the feasible region of power flow approximations does not enclose the feasible space of the non-convex problem. Hence, the global optimality of an approximated power flow problem solution cannot be guaranteed [36]. Semidefinite Programming (SDP) Relaxation and Second-Order Conic Programming (SOCP) Relaxations are the main methods utilized in the literature. SOCP was utilized in this paper to convexify the power flow equations due to the limited guarantee of the exactness of SDP

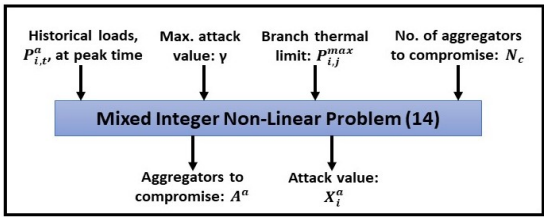

Fig. 6. High level flowchart of inputs and outputs of mitigation scheme

to only a certain class of problems with certain assumptions. Moreover, SOCP has been demonstrated in the literature to have a computational advantage over SDP [37].

SOCP relaxation of the power flow equations involves the introduction of new variables representing the product of voltages. Given voltage at bus i is represented in rectangular coordinates as $V_i = V_{di} + jV_{qi}, \forall i \in N_d$, the squared voltage magnitude is represented by c_{ii}. New variables c_{ij} and s_{ij} are introduced to represent the real and imaginary parts of the product of voltages at bus i and its conjugate at bus j respectively, $\forall\{i,j\} \in N_d$. Using these new variables, the power flow equations (6) are changed as,

$$\begin{aligned} P_i^G - P_i^L &= c_{ii}G_{i,i} + \sum_{j\neq i}^{N_{bus}} \Big(c_{ij}G_{i,j} - s_{ij}B_{i,j}\Big) \\ Q_i^G - Q_i^L &= -c_{ii}B_{i,i} + \sum_{j\neq i}^{N_{bus}} \Big(-c_{ij}B_{i,j} - s_{ij}G_{i,j}\Big) \end{aligned} \tag{17}$$

The following constraints need to be added to the MINLP,

$$c_{ij} = c_{ji} \text{ and } s_{ij} = -s_{ij}, \forall\{i,j\} \in B \tag{18}$$

$$c_{ij}{}^2 + s_{ij}^2 = c_{ii}c_{jj}, \forall\{i,j\} \in B \tag{19}$$

where B is the set of lines in the sub-network. By changing the equality constraint to inequality as illustrated in (20), the power flow equations are a form of SOCP and are now convex.

$$c_{ij}{}^2 + s_{ij}{}^2 \leq c_{ii}c_{jj}, \forall\{i,j\} \in B \tag{20}$$

Hence, replacing (6) with (17-18) and inequality constraint (20) results in MINLP (21) that needs to be solved and checked for exactness. If the solution for (21) satisfies (19) then the solution is global.

$$\begin{aligned} &\min \sum_{a\in N_a}\sum_{i\in N_d} X_i^a \\ &\text{s.t. (9), (13), (15-16), (17-18), and (20)} \end{aligned} \tag{21}$$

D. Using Generalized Bender Decomposition (GBD)

To solve the MINLP (21), GBD [38] was utilized. The basic idea in GBD is dividing the MINLP into two parts: the primal and the master problem. The primal problem involves fixing the y binary variables such that the problem is now only in the x-space. y represents A^a which is an array of N_a binary variables. x represents the n continuous variables in our optimization problem. Hence, $x = \{P_i^G, Q_i^G, P_{i,j}, \Delta_i^a, X_i^a, c_{ij}, s_{ij}\}$. The MINLP is reduced now to a nonlinear problem that can be solved using any of the commercial solvers to determine the x continuous variables. The solution obtained from the primal problem represents the upper bound solution for MINLP (21). The master problem then utilizes the obtained Lagrange multipliers and the x variables solution from the primal problem to change the problem to a MIP determining y. The solution for the master problem would then represent the lower bound of the global solution. The process is repeated between the primal and the master problem until the sequences converge. Figure 7 illustrates the steps involved in executing the GBD algorithm to solve the optimization problem.

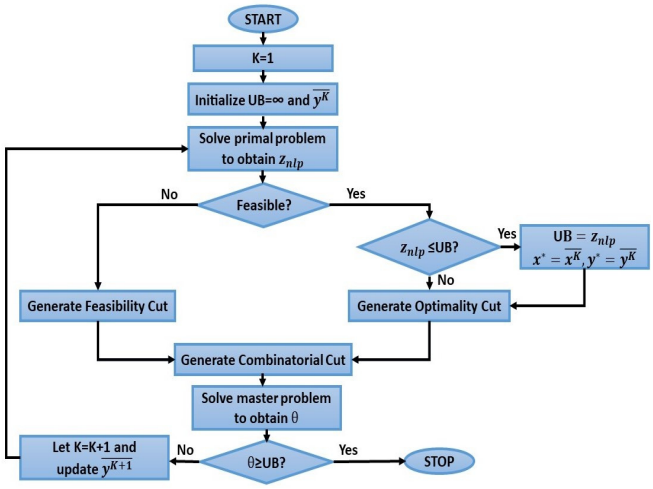

Fig. 7. Generalized Bender Decomposition Flowchart

E. Case Study Results

The proposed mitigation scheme was tested on the IEEE 33 case study which was assumed to be compromised using LAAs. For identifying the most critical aggregator in the network, N_c (13) was set to 1. GBD resulted in identifying aggregator 7 as the optimal aggregator to attack with a minimal attack value, X_i^a, of 0.1762. Thus, to ensure a stealthy attack, an adversary's first choice of attack to cause congestion during peak time is to attack aggregator 7. This is a realistic choice since commercial bus 7 is at peak load at that time, having an FCDC parking lot, compared to the other buses. Hence, the security of aggregator 7 needs to be reinforced. For a multi-point attack, where N_c (13) was set to 2, GBD resulted in identifying aggregators 6 and 7 as the optimal choice for being compromised with a maximum attack value, X_i^a, of 0.095. On the other hand, for a multi-point attack where $N_c = 3$, aggregators 3, 6, and 7 were identified as critical aggregators that would require the minimum amount of load scaling of 0.054 to achieve a stealthy attack. All the solutions obtained were observed to be exact on testing using the equality constraint (19). Hence, security reinforcement of aggregators 3, 6, and 7 would mitigate a LAA that aims to create congestion in the network.

For an adversary that aims to hide congestion, the GBD algorithm was executed on MINLP (21) with negative γ. Also, the power flow in the branch is ensured to be lesser than its maximum limit. For identifying the most critical aggregator in the network, N_c (13) was varied between 1 to 3. The optimization problem resulted in identifying aggregator 7 as the critical aggregator that needs to be secured in the event of a single point attack. On the other hand, for a multi-point attack, the optimization problem resulted in identifying aggregators 3, 6, and 7 as the three most critical aggregators in the network. These aggregators are capable of achieving the objective of the cyber attackers with an attack value, X_i^a, as low as -0.17. All the solutions obtained were observed to be also exact on testing using the equality constraint (19). Hence, security reinforcement of aggregators 3, 6, and 7 would mitigate a load altering cyber attack that aims to create congestion, increase existing congestion, or hide congestion in the network.

F. Computational Scalability

To test the scalability of the proposed mitigation scheme, the performance of the algorithm was tested on the IEEE 70 bus system [31]. As illustrated in Table VI, using GBD to determine the critical aggregator in the network that needs to be secured, the number of variables in the master problem depends on the number of aggregators. In the current case scenario, 9 aggregators were used to represent both networks. Also, the number of variables and constraints in the primal problem of the IEEE 70 system is nearly double that of the IEEE 33 bus system. This, however, did not have a large effect on the time required to determine the critical aggregators.

G. Discussion

To decrease the attack value, X_i^a, required to create or hide congestion while ensuring its stealthiness, a multi-point attack is more effective than a single point attack. In a multi-point attack, the attacker is capable of distributing the change in load needed to achieve its objective to more aggregators. However, as the number of aggregators compromised increases, the complexity of performing the attack without being detected also increases. Hence, N_c was restricted to only determining the first three critical aggregators. Moreover, for a single point attack, as the security of the first critical aggregator was reinforced, X_i^a required to compromise the second most critical aggregator increases risking the stealthiness of the attack. Aggregators 3, 6, and 7 were the adversary's first choices of attack. Hence, their security needs to be reinforced to prevent LAA. Compromising other aggregators would require the attacker to increase X_i^a to larger values or increase the aggregators compromised risking the stealthiness of the attack. To simulate this scenario, a constraint was added to MINLP (21) preventing aggregators 3, 6 and 7 from being identified as critical. Instead, simulating a single-point attack, resulted in identifying aggregator 4 as the next critical aggregator with an attack value of 0.659. However, to compromise aggregator 7, an attack value of 0.1762 was needed to achieve the objective of the attacker. This increase in attack value by more than 200% would affect the stealthiness of the attack. For a multi-point attack, aggregators 2, 3 and 4 were identified as the next set of critical aggregators with a maximum attack value of 0.09. Hence, the attack value increased by 66.67% which increases the chance of it being detected by the DNO. This mitigation scheme needs to be executed by the DNO whenever a new aggregator is introduced in the network, or when any of the aggregators have a major change in their loads (for example installation of EV charging parking lots).

TABLE VI
COMPUTATIONAL SCALABILITY OF MITIGATION SCHEME

Description	IEEE 33	IEEE 70
No. of variables to solve primal subproblem	398	818
No. of constraints to the primal subproblem	458	926
No. of variables to solve master problem to	9	9
Execution time	6.411 sec	6.679 sec

V. CONCLUSION

The reliance of market-based congestion management methods on the communication layer makes them vulnerable to cyber attacks, as investigated in this paper. The impact of Load Altering Attacks (LAA) on such congestion management techniques, as a result of attackers utilizing cyber vulnerabilities, were studied. Two optimization problems were developed to determine the minimum number of aggregators needed to be attacked to create or hide congestion in the distribution network. IEEE 33 bus system was used as a case study to evaluate the impact of LAAs on network congestion and electricity price. Mixed Integer Non-Linear Programming was used to determine the aggregators to compromise to achieve a cyber attacker's objective. A stealthy attack that creates and/or increases congestion, caused the DNO to impose a congestion tariff higher by 14.4% to motivate consumers to reduce their demand at congestion times. This tariff results in larger electricity bills which eventually would be paid by unhappy consumers. On the other hand, compromising aggregators to hide congestion caused the DNO to not impose any congestion tariff. This results in the network operator having to deal with the congestion in real-time.

Cyber security of various entities involved in indirect congestion management techniques is vital for congestion relief. A mitigation scheme was developed to determine the critical aggregators in the network that requires minimal attack values to either fake or hide congestion. Security for these critical aggregators needs to be reinforced to mitigate stealthy LAAs in the day-ahead market. Future work aims to study the effect of other attacks on DSM-based congestion management methods and developing one mitigation scheme for all.

ACKNOWLEDGMENT

This work is supported by the CIRA-013-2020, Khalifa University, U.A.E.

REFERENCES

[1] T. Vo, A. Haque, P. Nguyen, I. Kamphuis, M. Eijgelaar, and I. Bouwman, "A study of congestion management in smart distribution networks based on demand flexibility," in *IEEE Manchester PowerTech*, 2017, pp. 1–6.
[2] "IEEE guide for loading mineral-oil-immersed transformers and step-voltage regulators," *IEEE Standard C57.91-201*, 2012.
[3] "IEC loading guide for oil immersed power transformers," *IEC Standard 60076-7*, 2005.
[4] S. Huang, Q. Wu, H. Zhao, and C. Li, "Distributed optimization based dynamic tariff for congestion management in distribution networks," *IEEE Transactions on Smart Grid*, 2018.
[5] Y. Gu, J. Xie, X. Chen, K. Yu, Z. Chen, and Z. Li, "Dynamic tariff method for congestion management in distribution networks," in *IEEE Conf. on Energy Internet and Energy System Integration*, 2017, pp. 1–6.
[6] S. Huang and Q. Wu, "Dynamic subsidy method for congestion management in distribution networks," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 2140–2151, May 2018.
[7] A. Kulmala, M. Alonso, S. Repo, H. Amaris, A. Moreno, J. Mehmedalic, and Z. Al-Jassim, "Hierarchical and distributed control concept for distribution network congestion management," *IET Generation, Transmission Distribution*, vol. 11, no. 3, pp. 665–675, 2017.
[8] S. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: Vulnerabilities, threats and countermeasures," *IEEE Transactions on Industrial Informatics*, 2019.
[9] T. S. Ustun and S. M. S. Hussain, "A review of cybersecurity issues in smartgrid communication networks," in *2019 International Conference on Power Electronics, Control and Automation*, 2019, pp. 1–6.

[10] K. Jhala, B. Natarajan, A. Pahwa, and H. Wu, "Stability of transactive energy market-based power distribution system under integrity attack," *IEEE Trans. on Industrial Informatic*, vol. 15, pp. 5541–5550, 2019.
[11] H. Karimi, K. Jhala, and B. Natarajan, "Impact of real-time pricing attack on demand dynamics in smart distribution systems," *NAPS*, 2018.
[12] U. Anubunwa, H. Rajmani, R. AbdAlhamed, and P. Pillai, "Investigating the impacts of cyber-attacks on pricing data of home energy management systems in DR programs," in *IEEE PESGM*, 2018, pp. 1–5.
[13] A. 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, 2011.
[14] S. Amini, F. Pasqualetti, and H. M. Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, pp. 2862–2872, 2018.
[15] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014.
[16] C. Lai, N. Jacobs, S. Hossain-Mckenzie, C. Carter, P. Cordeiro, I. Onunkwo, and J. Johnson, "Cyber security primer for DER vendors, aggregators, and grid operators," 2017.
[17] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, 2014.
[18] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2017.
[19] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1802–1810, 2017.
[20] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2038–2049, 2016.
[21] S. Wang, W. Ren, and U. M. Al-Saggaf, "Effects of switching network topologies on stealthy false data injection attacks against state estimation in power networks," *IEEE Systems Journal*, vol. 11, 2017.
[22] Z. Zhang, R. Deng, D. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Trans. on Information Forensics and Security*, 2020.
[23] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices," *IEEE Trans. on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, 2020.
[24] S. Huang, Q. Wu, L. Cheng, and Z. Liu, "Optimal reconfiguration-based dynamic tariff for congestion management and line loss reduction in distribution networks," *IEEE Trans. on Smart Grid*, vol. 7, 2016.
[25] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "Can attackers with limited information exploit historical data to mount successful FDI attacks on power systems?" *IEEE Trans. on Power Systems*, vol. 33, 2018.
[26] A. Ayad, M. Khalaf, and E. El-Saadany, "Cyber-physical security of state estimation against attacks on wide-area load shedding protection schemes," in *IEEE ISGT Conference*, February 2019, pp. 1–5.
[27] K. Khanna, B. Panigrahi, and A. Joshi, "Bilevel modelling of false data injection attacks on security constrained optimal power flow," *IET Generation, Transmission Distribution*, vol. 11, pp. 3586–3593, 2017.
[28] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Transactions on Power Delivery*, vol. 4, no. 2, pp. 1401–1407, April 1989.
[29] E. A. Rezai, M. Shaaban, E. F. El-Saadany, and F. Karray, "Online intelligent demand management of plug-in electric vehicles in future smart parking lots," *IEEE Systems Journal*, vol. 10, pp. 483–494, 2016.
[30] G. D. Corporation, "Gams release 24.2.1," Washington, DC, USA, 2013.
[31] D. Das, "A fuzzy multiobjective approach for network reconfiguration of distribution systems," *IEEE Trans. on Power Delivery*, vol. 21, no. 1, pp. 202–209, 2006.
[32] "Overcurrent protection," *National Electrical Code Article 240*, 2017.
[33] S. Huang, Q. Wu, Z. Liu, and A. Nielsen, "Review of congestion management methods for distribution networks with high penetration of DERs," in *IEEE PES Innovative Grid Technologies*, 2014, pp. 1–6.
[34] M. Shabanzadeh, M. Eslami, and M. Haghifam, "Risk-based medium-term trading strategy for a vpp with first-order stochastic dominance constraints," *IET Generation, Transmission Distribution*, vol. 11, 2017.
[35] R. A. Jabr, "Radial distribution load flow using conic programming," *IEEE Transactions on Power Systems*, vol. 21, 2006.
[36] D. K. Molzahn and I. A. Hiskens, *A Survey of Relaxations and Approximations of the Power Flow Equations*, 2019.
[37] B. Kocuk, S. Dey, and X. Sun, "Strong SOCP relaxations for the optimal power flow problem," *Operations Research*, vol. 64, p. 1177–1196, 2016.
[38] M. Kılınç and N. Sahinidis, "Exploiting integrality in the global optimization of mixed-integer nonlinear programming problems with baron," *Optimization Methods and Software*, vol. 33, pp. 1–23, July 2017.

Omniyah Gul M Khan received the B.Sc. and M.Sc degrees in Electrical Engineering from the American University of Sharjah, Sharjah, U.A.E in 2008 and 2010 respectively. She is currently working toward the Ph.D. degree from the Electrical and Computer Engineering Department, University of Waterloo, Waterloo, ON, Canada. Her research interests include demand side management, cyber security of distribution systems and artificial intelligence.

Ehab F. El-Saadany (SM'05) was born in Cairo, Egypt, in 1964. He received the B.Sc. and M.Sc. degrees in electrical engineering from Ain Shams University, Cairo, Egypt, in 1986 and 1990, respectively, and the Ph.D. degree in electrical engineering from the University of Waterloo, Waterloo ON, Canada, in 1998, where he was a Professor in the ECE Department till 2019. Currently, he is a Professor in the Electrical and Computer Engineering Department and the Director of the Advanced Power and Energy Research Center at Khalifa University, Abu Dhabi, UAE. His research interests include smart-grid operation and control, microgrids, self healing, power quality, distributed generation, power electronics interfacing, and mechatronics. He is a Registered Professional Engineer in the Province of Ontario, Canada.

Amr Youssef (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees from Cairo University, Cairo, Egypt, in 1990 and 1993, respectively, and the Ph.D. degree from Queens University, Kingston, ON, Canada, in 1997. He worked for Nortel Networks, the Center for Applied Cryptographic Research, University of Waterloo, IBM, Armonk, and Cairo University. He is currently a Professor with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC, Canada. His research interests include cryptology, malware analysis, and cyber-physical systems security. He has more than 230 referred journal and conference publications in areas related to his research interests. He also served on more than 60 technical program committees of cryptography and data security conferences.

Mostafa F. Shaaban (SMIEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from Ain Shams University, Cairo, Egypt, in 2004 and 2008, respectively, and the Ph.D. degree in electrical engineering from the University of Waterloo, Waterloo, ON, Canada, in 2014.
Currently, he is an associate professor in the Department of Electrical Engineering, American University in Sharjah, Sharjah, United Arab Emirates, and adjunct with University of Waterloo, Waterloo, ON, Canada. Dr. Shaaban has several publications in international journals and conferences and serves as an associate editor for IET smart grid and a reviewer for several refereed journals. His research interests include smart grid, renewable DG, distribution system planning, electric vehicles, storage systems, and bulk power system reliability.