Contextual Dishonest Behaviour Detection for Cognitive Adaptive Charging in Dynamic Smart Micro-Grids

Milena Radenkovic
School of Computer Science
The University of Nottingham
Nottingham, NG8 1BB, UK
milena.radenkovic@nottingham.ac.uk

Adam Walker
School of Computer Science
The University of Nottingham
Nottingham, NG8 1BB, UK
adam.walker4@nottingham.ac.uk

***Abstract*— The emerging Smart Grid (SG) paradigm promises to address decreasing grid stability from thinning safe operating margins, meet continually rising demand from pervasive high capacity devices such as electric vehicles (EVs), and fully embrace the shift towards green energy solutions. At the SG edge, widespread decentralisation of heterogeneous devices coupled with fluctuating energy availability and need as well as a greatly increased fluidity between their roles as energy producers, consumers, and stores raises significant challenges to ensuring robustness and security of both information and energy exchange. Detecting and mitigating both malicious and non-malicious threats in these environments is essential to the realisation of the full potential of the SG. To address this need for robust, localised, real-time security at the grid edge we propose CONCEDE, a collaborative cross-layer ego-network integrity awareness and attack impact reduction extension to our previous work on delay-tolerant cognitive adaptive energy exchange. We detail a substantial, targeted, energy disruption attack perpetrated by colluding mobile energy prosumers. Our CONCEDE proposal is then evaluated in multiple, diverse smart micro-grid (SMG) scenarios using hybrid traces of EVs and infrastructure from Europe, North America, and South America in the presence of a coordinated attack from malicious distributors seeking to disrupt energy supply to a target community. We show that CONCEDE successfully detects and identifies the nodes exhibiting malicious, dishonest behaviour and that CONCEDE also reduces the impact of a coordinated energy disruption attack on innocent parties in all explored scenarios across multiple criteria.**

Keywords*— *Smart energy, Mobile DTNs, Autonomous Vehicles, Security

I. INTRODUCTION

Evolving energy conditions worldwide are necessitating a global redressing of the conventional electrical grid model. In developed nations, perpetually rising energy demand combined with the ongoing shift away from fossil-fuel power is exhausting capacity margins and it is anticipated that the near-future hike in demand driven by widespread charging of electric vehicles (EVs) will push the grid beyond its limits[2]. At the same time, in many developing countries there is limited grid penetration and the already unreliable electrical infrastructure is unable to meet rising consumer demand and remain secure in the face of substantial losses due to significant energy theft and infrastructure inefficiencies [3]. The future smart grid (SG) and smart micro-grid (SMG) paradigms are high priority interdisciplinary research areas which aim to reconcile these issues, promising distributed, collaborative, and adaptive energy management through deep integration of highly heterogeneous devices, ranging from smart home appliances to autonomous EVs [4]. Despite widely acknowledged benefit to industry and consumer stakeholders alike, realisation of the SG necessitates robust, responsive communications systems providing for availability, pricing, and usage information exchange as well as for coordination and collaboration between edge devices and the wider grid. Providing secure and robust communications and energy transfer systems in the presence of both emerging malicious and non-malicious threats is fundamental to the success of the future SG [5]. Many state-of-the art approaches are investigating this area, e.g. [6].

Consumer EVs and industry EV fleets will represent a core component of the future SG [7]–[9], having the potential to physically move energy in-network via localised opportunistic and on-demand energy transfer. We consider localised, delay tolerant bi-directional V2V and V2G energy and information exchange approaches integral to addressing the concerns of real-time adaptability, responsiveness, robustness, and fairness in the face of transient availability and dynamic energy supply and demand patterns in mobile SMGs. Centralised systems typically assume a priori knowledge and have been seen to be sub-optimal, unfair, insufficiently real-time, and inadequately tolerant to localised faults and network disruption [10]–[13]. To overcome the limitations of centralised approaches, we proposed CognitiveCharge [14], a fully-distributed, disconnection-tolerant, multi-layered predictive analytics suite and combined utility heuristic-driven approach for opportunistic vehicle-to-vehicle (V2V) and vehicle-to-grid (V2G) energy and information transfer in heterogeneous dynamic SMGs. CognitiveCharge analytics allow for nodes to avoid both under and overutilisation of energy resources, preventing exploitation of nodes, regions, and communities. As such, CognitiveCharge nodes adapt in real-time to the dynamic temporal network conditions of EV mobility and fluctuating, transient energy availability and power needs of both EVs and static infrastructure.

In this paper we propose CONCEDE which builds on and extends our multi-dimensional CognitiveCharge approach to enable it to operate reliably in the face of malicious or dishonest nodes. CONCEDE seeks to meet the challenges of providing robust SG energy and information communications through addition of a novel, collaborative cross-layer malicious misbehaviour detection and attack mitigation scheme. CognitiveCharge [14] nodes are robust to highly dynamic network conditions; for example, in the case of an unexpected regional energy blackout, risk of depletion to affected nodes is reduced as energy is adaptively moved in a multi-hop manner from nodes and regions with surplus to those in deficit regions. Robustness of CognitiveCharge is

ISBN 978-3-903176-13-3

dependent upon collaborative dissemination and propagation of honest, accurate information. CONCEDE extends CognitiveCharge by allowing nodes to detect and respond in real-time to threats to themselves and their community from both malicious and faulty malfunctioning nodes, permitting more informed, responsive energy related decisions even in the presence of misbehaviour and dishonesty. More specifically, CONCEDE combines CognitiveCharge predictive local and ego-network multi-layer predictive analytics [14] with the ability to scrutinise the behaviour of nodes in their ego-network and additionally discern when exchanged information is incorrect or falsified.

The remainder of this paper is structured as follows. In Section II we give an overview of related work and existing proposals for robust V2V and V2G information and energy exchange. Our heterogeneous mobile SMG environment and threat model are described in Section III. In Section IV we describe our proposal for CONCEDE, our contextual integrity awareness for security aware CognitiveCharge, giving a high level architectural overview, highlighting the wider integration within CognitiveCharge framework, and detailing the collaborative predictive multi-layer heuristic-based decision making process. Section V discussed our evaluation of CONCEDE in multiple heterogeneous dynamic SMG scenarios using multi-layered hybrid real-world and pseudo-realistic traces for Nottingham, Paris, Rio de Janeiro, and San Francisco, as well a synthetic Manhattan model. Our results show that CONCEDE nodes successfully detect and collaboratively reduce the impact of an energy disruption attack conducted by coordinated energy prosumers. Conclusions are drawn in the final section together alongside a discussion of future work.

II. Related Work

Research and experimental activity conducted by the Danish EDISON project on the island of Bornholm has evaluated the benefits of large EV fleets to both vehicle owners and the operation of the wider grid [15]. The distributed software and ICT aspects of V2G integration were a particular focus in [15], which proposed the EDISON EV virtual power plant (EVPP) where EV fleets integrated with the grid to stabilise wind renewable energy resources .

A number of other works have explored various aspects of energy as a tradable commodity directly between EVs and with the wider grid for a range of benefits. In [16] a peer-to-peer trading system for direct energy exchange amongst edge devices is proposed for consumers to source geographically local available supply from others offering their surplus charge. A localised authentication mechanism for V2V charging is explored in [17] which proposes a challenge-response protocol between EVs.

AdaptAnon [18] is a multidimensional k-anonymity approach for dynamic, heterogeneous opportunistic networks which adaptively balances the degree of obfuscation with performance to achieve a high diversity of nodes in multi-hop paths at minimal cost to success ratios and delays. OCOT-AA [19] builds upon AdaptAnon with a robust, fully-distributed, self-organised reputation mechanism and collaborative opportunistic testing technique to provide full source anonymisation when even a large proportion of nodes are malicious. Approaches to location privacy using k-anonymity techniques in mobile opportunistic networks are proposed in [20]. We build upon these techniques but diverge in our consideration of user requirements. In this paper we deem collaboration advantageous rather than strictly necessary due to the real-time nature of energy supply and demand.

Vehicular networks are inherently disconnection-prone and highly dynamic due to their fast changing topologies resulting from vehicle mobility patterns. V2V and V2G dynamic charging necessitates stringent responsiveness and availability demands in order to facilitate robust adaptive, real-time, collaborative decision making. Existing works are largely dependent on coordination of vehicles through a remote centralised authority with which they are typically assumed to communicate with via cellular networks (e.g. [21], [22]). Under such conditions, attaining global optimum using centralised optimisation have been shown to be unsuitable as they disadvantage some parties and nodes can be unfairly exploited [10], [11]. In SMG scenarios this exploitation could be both monetary and energy related - in the worst case depleting a node unfairly for another's benefit. In temporally changing complex graph topologies, collaborative approaches have been shown to outperform centrally and locally optimised algorithms [11].

The social integration requirements and impact of misrepresentation attacks in opportunistic network environments was explored in [23], where a number of novel mitigation strategies were proposed. [23] additionally showed the high complexity requirements for malicious, lying and potentially colluding nodes to join an established social group.

III. Coordinated Energy Disruption Attack in Dynamic Smart Micro-Grids

This section provides a detailed description of our SMG scenario and gives an overview of a targeted coordinated energy disruption and DoS attack in a SMG environment. We also contextualise the scope and severity of the threat scenario in the real-world by providing several compelling examples of attacker motivations.

A. Heterogeneous Mobile Smart Micro-Grid Environment

We explore a distributed, dynamic SMG environment comprising highly heterogeneous mobile and static nodes at the SG edge participating in localised energy exchange. Nodes consume energy via conventional means (e.g. mobility, communications, computation) in addition to offloading and acquire energy directly from other nodes including EVs and the grid (e.g. at infrastructure charge-points). Though the roles of all nodes in the SMG (e.g. consumer, producer, supplier, distributor) are dynamic and fluctuate in real-time depending upon local energy state and node operation at a given moment in time, for better illustrating our scenario we broadly categorise nodes based upon their dominant behaviour. As shown in Fig. 1, similar nodes can be grouped based on multiple factors, including mobility, capacity, and general energy availability behaviour. Using this categorisation, nodes in our SMG scenario are considered to be either suppliers, prosumers, or distributors.

- **Distributors**: Mobile nodes which routinely carry surplus energy for exchange at dynamic, locally calculated market prices are considered distributors. These nodes acquire energy from infrastructure and then offload it amongst needy consumers (i.e. as customers) for profit. We consider distributors to be mobile nodes with high storage capacity dedicated to

ISBN 978-3-903176-13-3 © IFIP

providing electricity to consumers who are largely made up of limited capacity mobile SMG devices.

- **Prosumers**: Mobile SMG edge devices (e.g. autonomous EVs) with high fluctuation between supply and demand behaviour are considered prosumers in our scenario. Like distributors, prosumers have on-board battery storage and both consume and supply electricity through direct, bidirectional energy exchange. When in energy surplus, a prosumer can choose to offload energy by selling it to nodes in deficit. Conversely, a prosumer in need (or anticipating future need) of energy can seek to acquire charge from nodes with surplus.
- **Suppliers**: Energy sources such as homes and public infrastructure EV charge-points are considered suppliers in our scenario. Nodes in this group are largely static and have high energy availability for dissemination. Suppliers receive large amounts of energy directly from the upstream grid and can support local generation. Suppliers may opportunistically take advantage of available prosumers and distributors for grid stabilisation, opportunistic cost reduction, and to maintain uptime during periods of grid outage.

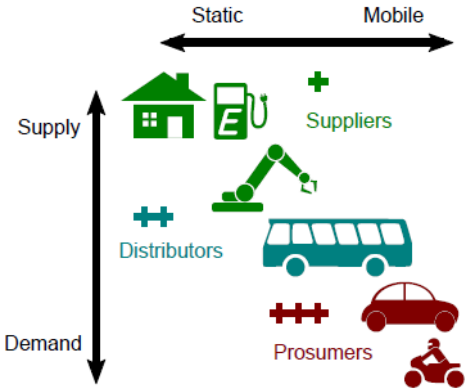

Fig. 1. Heterogeneous SMG nodes broadly grouped by majority energy availability, mobility dynamics, quantity, and capacity.

Our distributed and decentralised SMG scenario is modelled as a partially connected complex temporal network of distributors $D = \{d_0, d_1, \dots\}$, suppliers $S = \{s_0, s_1, \dots\}$, and prosumers $P = \{p_0, p_1, \dots\}$ represented by a graph with time varying edges $G = (V, E)$ where $V = D \cup P \cup S$. In the baseline CognitiveCharge [14] scenario, every node monitors its own resource availability across multiple criteria and periodically exchanges this information, combined with its self-identified energy state (i.e. seek, supply, store), with directly adjacent vertices $N_{(G,t)}(v)$. These status messages in conjunction with local, real-time coordination of supply and demand allow for distributed energy exchange with the most needy nodes being supplied by the nodes with highest capacity. Using these perceived analytics and utility measure information, nodes are able to make real-time, localised energy exchange decisions, i.e. supply, acquire, or store. For example, a prosumer in need of energy and in contact with an available supplier may seek to acquire charge from it.

B. Threat Model

The particular threat that forms the focus of this work is a targeted, coordinated energy disruption and DoS attack conducted by colluding mobile energy prosumers. We consider a malicious or hacked energy prosumer who wishes to disrupt the supply of energy to a region, cause grid instability and deny energy access to nodes in a target area. The disruption of energy supply to a community may potentially cause complete temporal isolation from established supply chains (e.g. terrorism causing targeted blackouts) as well as additional profiteering. Nodes in the energy isolated area with one distributor may face imminent depletion if newly malicious prosumer buys all the energy. Rival distributing or supplying companies could also conduct such an attack in order to effectively 'evict' competing energy providers and drive up profits for themselves.

In order to carry out the energy disruption attack, the attacker gains control (e.g. through remote hacking or via legitimate ownership) of several existing distribution nodes and uses them to launch a coordinated energy disruption attack. The malicious energy prosumer disseminates falsified information pertaining to local energy usage, demand, availability and pricing. The aim of this misrepresentation is for the attacker to embed itself in the local network by either 1) seeking more energy than it actually needs in order to deplete the distributors or 2) promoting itself as the desirable, available energy supplier and simultaneously demoting the local perception of other providers.

An overview of several attack types in this context is shown in Fig. 2 using a subset of a SMG scenario comprising distributors (d_0, d_1), prosumers (p_0, p_1), and a single malicious node m. For a connected SMG graph G the community $\{d_0, d_1, p_0, p_1\}$ is a sub-graph H where $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.

In Fig. 2.1, the SMG is operating in a steady-state with both of the prosumers low on energy acquiring charge opportunistically at an accepted price from adjacent distributors with surplus. Through both eavesdropping and behavioural analysis of nodes in its neighbourhood $N(m)$, the malicious node passively identifies the vulnerable community H as the target of attack due to limited connectivity with wider grid infrastructure in G and a reliance on just few distributors.

Fig 2.2 shows a node m that proactively disseminates falsified resource availability messages to nodes in its vicinity with the intent of actively disrupting energy supply to the target region. The falsified messages sent differ depending upon the identified energy state of the recipient in order to maximise the impact of the attack. To peer distributors and suppliers $N_d(m)$, m aims to demote the utility of nodes in $N_p(m) \cup N_s(m)$ as potential consumers, preventing further energy from being delivered to the target region. This can be accomplished in a range of ways, for example, by directly advertising that that these nodes are not in need of energy or by falsely claiming that they have high availability at lower cost than the distributors are offering. In doing this, distributors with insufficient evidence to the contrary will offload energy to other regions with higher perceived need at an offering price believed to be better. Falsified messages sent to nodes in $N_p(m)$ seek to raise the utility of m as an energy source for later exploitation, increase reliance on m, and mitigate attempts at acquisition from alternate sources in G.

Fig. 2.3 highlights that m has successfully promoted the utility of itself as an energy seeker over p_0 and p_1, thus directly exhausting community distributor supplies and preventing energy from reaching the truly needy prosumers.

ISBN 978-3-903176-13-3

Though the attacker pays honestly for energy, in manipulating the perception of energy availability the price paid will likely be at most the same as that previously paid by p_0 and p_1. In a temporal attack the price can even be significantly lower due to the distributors seeking to offload surplus originally intended for the prosumers.

Fig 2.4 shows how the exhausted region can be further exploited through the attacker offloading overpriced energy to the increasingly desperate nodes (i.e. p_0, p_1.). The attacker promotes itself as the desired supplier to nodes who face critical depletion levels (or even complete loss of energy) if they do not acquire energy but have no alternative available providers. Node m can charge increased prices for its energy supply.

This form of energy disruption attack is particularly effective as once energy has been exchanged by a malicious mobile consumer, it is not recoverable until a future acquisition opportunity arises. Similarly, once energy has been obtained to satisfy the immediate needs of a malicious consumer, it will not seek to charge again until it needs to, regardless of later detected better alternatives. The attacker can further maximise the impact by targeting vulnerable communities which are already particularly isolated and peripheral to the SG.

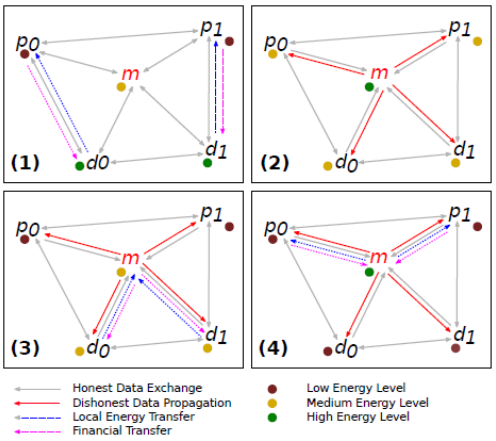

Fig. 2. Attack overview: (1) Steady-state scenario. (2) Malicious distributor disseminates falsified availability messages. (3) Distributors supply malicious distributor instead of seekers. (4) Depleted prosumers must charge from malicious distributor.

The cost for a malicious node to integrate itself into an established social community can be particularly high because in order to exert negative influence over the community, the new malicious node must build and maintain genuine connections with highly influential uncompromised nodes [23]. Rather than deploy new malicious nodes or risk direct association with the attack, an alternative option for an attacker is to gain temporary control over honest nodes and exploit the trust already placed in them nodes by others in the community. The attacker can then move its fully honest nodes with high energy surplus into the target region for the final price-gouging step, successfully conducting the attack and retaining its trust in the event of future detection of m.

IV. COGNITIVE ADAPTIVE CHARGING WITH CONTEXTUAL DETECTION OF DISHONEST BEHAVIOUR

We propose CONCEDE, a novel threat detection and mitigation scheme for the SMG which uses multi-layer, multi-dimensional, local and ego-network predictive contextual integrity awareness analytics to extend CognitiveCharge [14] – our multi-layer disconnection-tolerant cognitive adaptive charging approach for V2V and V2G energy exchange.

We model the network as a temporal graph $G = (V, E)$ where the connectivity of the network edges E and the state of nodes V change over time. Each of these is modelled as a time series set with vertices depicted as $V = \{V_t | t \in T\}$ and edges as $E = \{E_t | t \in T\}$, where t is a member of the time series T. We assume that connectivity is bidirectional and therefore the edges of the graph are undirected, thus the temporal edge connecting nodes a and b at time t $(a, b \in V_t)$ we denote as $\{u, v\} \in E_t$. A path we model as a sequence of time variant energy supply and demand locations where each index represents a particular time interval, e.g. path $Q = (e_0, e_1, \dots, e_k)$ where $e_i = \{v_{i-1}, w_i\}$ for $v, w \in E$.

While energy is stored in a node without the node using it (either for its mobility or transferring to the other nodes), efficiency of the network energy resources is reduced, and it is more efficient for energy to be transferred via a number of hops with smaller in-network delays in order to arrive at the destination where it is in demand. Note that there is a considerable time variation between the energy system speeds and node mobility with charging and communications being much faster than the speed of mobile nodes. However, there is a strong spatiotemporal correlation between time-variant supply-demand layer and the mobility layer which our approach is able to capture, model and adapt to. For example, the faster the nodes move, the higher the demand they place on energy; the higher the number of moving collocated nodes, the higher the demand of that region. We define resource consumption as dynamic subgraph $G' = (V', E')$ where the set of vertices are defined as the set of vertices with demand greater than 0 $(V' = \{\forall v_t \in V : D_v^t > 0\})$ and the set of edges is defined as the set of edges that have a demand greater than 0 $(E' = \{\forall e_t \in E : D_e^t > 0\})$. The combined geo-temporal connectivity graph G and the spatiotemporal graph of consumed and needed resources G' is depicted as $U = \frac{|G'|+\|G'\|}{|G|+\|G\|}$.

Fig 3 gives an overview of CognitiveCharge [14] and CONCEDE. The cognitive adaptive energy exchange decision making approach in CognitiveCharge uses a novel suite of fully-localised, predictive energy awareness analytics which are locally aggregated in real-time for both an independent node and its ego-network, namely: depletion rate, congestion rate, receptiveness, retentiveness, and dynamic energy pricing. These CognitiveCharge analytics build upon previous utility-driven decision making approaches [1][24][26] and use both first-hand and ego-network multi-layer analytics in order to describe the contextual, multi-criteria utility of itself and encounters for individual nodes, the neighbouring community, and surrounding geographic region. Through localised peer exchange of this individual and ego-network summary information, every CognitiveCharge node is able to use disseminated second-hand metrics to form aggregate analytics over its own ego-network. All CognitiveCharge nodes are therefore aware of their own current and forthcoming energy

needs and moreover are able to anticipate the energy-related behaviour, both individually and collectively, of nodes in its ego-network.

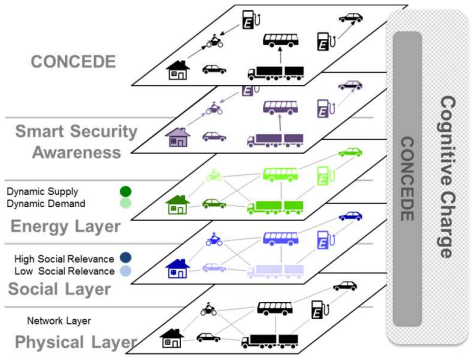

Fig. 3. CONCEDE architectural overview highlighting integration with CognitiveCharge and the cross-layer contextual information driving real-time energy and integrity aware decision making.

Fig. 3, shows CONCEDE architectural overview which, similarly to CognitiveCharge [14], receives inputs from each layer in order to extend the semantic knowledge of each node and uses this to further enhance the robustness of CognitiveCharge decision making. As previously described, CognitiveCharge is robust to dynamic energy conditions, however this adaptability is dependent upon honest information exchange. Contrary to this, CONCEDE proposal has ability to detect and adapt to inorganic conditions caused by faulty or malicious node behaviour.

The ego-network [1] graph for a node v can be represented by the sub-graph $Z_G(v)$ which contains the nodes immediately adjacent to v and their respective mutual edges, as shown in (1) (note that $N_G[v]$ denotes the closed neighbourhood of v). CONCEDE uses detected divergences in expected and actual ego-network resource as well a social connectivity awareness analytics (as calculated by CognitiveCharge [14]) to determine the integrity of a node with respect to its behaviour. This is conducted in real-time for all nodes and on aggregate for the ego-network, allowing for adaptive and robust decision-making regarding energy exchange.

$$V = N_G(v)$$
$$E' = \{v'v'' | v' \in V' \wedge v'v'' \in E_G(v') \wedge v'' \in N_G[v]\} \quad (1)$$
$$Z(v) = (V', E')$$

CONCEDE integrates with the analytics suite CC proposed in CognitiveCharge [14] where $CC = \{DR, CR, Rec, Ret, Price\}$. Node and ego network considerations allow nodes to adapt to a number of predictive analytics in order to:

- Avoid or charge less at the parts of the network with lower energy availability and higher depletion rates.

$$EN_{Ret}(X) = \frac{1}{N}\sum_{i=1}^{N} Ret(c_i(X)) \quad (2)$$

$$DR(X) = \frac{100\,\frac{T_{Cap}(X)}{T_{Total}(X)}}{\frac{1}{N}\sum_{i=1}^{N} Ts_i(X) - Te_i} \quad (3)$$

- Avoid or charge less at parts of the network with higher delays.

$$EN_{Rec}(X) = \frac{1}{N}\sum_{i=1}^{N} Rec(c_i(X)) \quad (4)$$

$$Rec(n) = \mu Rec_{old}(n) + (1-\mu) Rec_{current}(n) \quad (5)$$

- Avoid malicious nodes which are found to have a mismatch between what they are reporting and what the rest of the nodes observe and collaboratively predict about them.

Using moving average extrapolation, CONCEDE nodes calculate the anticipated value of each analytic for a given instant in time for a specific neighbour n. This is given as $e_a(n)_t$ (6) and determined using accurate calculations made previously from both direct observations and exchanged information.

$$e_a(n)_t = 2 \cdot a(n)_{t-1} - a(n)_{t-2} \quad (6)$$
$$d_{a,t} = |a(n)_t - e_a(n)_t| \quad (7)$$

The difference between the calculated, expected and determined actual analytic values $d_{a,t}$ (7) is then compared with an adaptive threshold difference level i for each analytic. The value i is dynamically adjusted in real-time based on the interval between calculations and available ego-network knowledge. By combining ego-network information with local knowledge, the threshold difference level is responsive to natural changes observed by independent nodes and neighbours (e.g. fluctuations in behaviour). Nodes with values exceeding i are considered to be dishonest and flagged as such until their perceived behaviour is in line with the information they are reporting to their peers. Simply blacklisting detected malicious or faulty nodes entirely is not always of benefit to CONCEDE nodes. For example, an energy consumer may still seek to use a dishonest node with real surplus in the case of poor local energy availability. Similarly, if a malicious node is advertising a need for energy but honestly willing to pay an acceptable price then CONCEDE nodes with surplus may still consider them as potential customers. To handle such scenarios, in addition to flagging CONCEDE allows for continued usage by extension of the CognitiveCharge decision making process, per (8) where $u(n)_t$ is expected to return a value in [0,1].

$$\text{CCUtil}(n)_t = \sum_{CC}^{u} u(n)_t - \frac{1}{0^{d_{u,t}(n)} + d_{u,t}(n)} \quad (8)$$

CONCEDE operation is therefore two-fold. Firstly, through collaborative information exchange, predictive analytics and first hand behaviour corroboration with anticipated CONCEDE nodes it can identify those determined to be propagating falsified information and consider them for protracted monitoring. The identity of these nodes and the associated recorded behavioural discrepancies are disseminated with the aggregate ego-network analytics for community resilience. Secondly, CONCEDE allows for usage of certain detected malicious nodes for energy exchange by identifying which, if any, behaviours are deemed honest. For example, a roaming malicious node acting maliciously in one location may act honestly in another. By including the weighting of the degree of dishonesty in the decision-making process, dishonest nodes, which may not be malicious and instead only temporally or partially faulty, can be considered for use.

V. Evaluation

In this section we discuss our multi-criteria evaluation of CONCEDE in the presence of multiple attackers using five

distinct hybrid real-world and pseudorealistic urban SMG scenarios using traces for Nottingham, UK [32]; Paris, France [32]; Rio de Janeiro, Brazil [30]; and San Francisco, USA [25] as well as a synthetic Manhattan grid model. We perform our experiments in ONE simulator [31] where 100 prosumer vehicles charging opportunistically are modelled over 5 days using real-world traffic patterns (San Francisco, Rio de Janeiro) and simulated workday patterns (Nottingham, Paris). Nodes communicate information via WiFi at a range of 100 metres with local charging conducted up to a maximum range of 10 metres. We use CogntiveCharge with no attack present as the baseline and compare this against CognitiveCharge in the presence of a malicious prosumer attack without defence and finally against CognitiveCharge with CONCEDE. CONCEDE is evaluated against existing work in the presence of sustained, active attack conducted temporally by multiple groups of mobile prosumers. After extensive analysis of our SMG scenarios we identified social-based community attacks to be more damaging than geographical region based attack models in terms of raw energy depletion from victims. Our evaluation of CONCEDE therefore focuses on malicious attackers targeting socially connected communities of nodes. We assume that the attacks are happening during the entire duration of the experiments.

The heterogeneous autonomous EVs in our scenarios are modelled from current consumer and commercial EVs and are all capable of participating in opportunistic V2V and V2G energy exchange. In addition to independent autonomous EVs exchanging surplus energy to those with deficit, in this paper we consider commercial vehicles with additional load capacity that are capable of acting as mobile energy distributors. These mobile distributors collaborate with consumer EVs in order to increase local availability. Consumer EVs are based on the current 2017 Smart ForTwo with a total 17.6 kWh capacity and approximate urban range of 100 km.

Traces devised for our Nottingham and Paris scenarios are pseudo-realistic and use a typical urban workday mobility pattern for commuter EVs. The Nottingham trace covers the unitary area of the city spanning 10.45 km x 14.18 km. A small, dense road-network lies at the core of the map surrounded by sprawling sub-urban residential regions connected via arterial roadways. Charge-points dominantly lie in the city centre with commuter traffic travelling to parking locations in this region on a daily basis. The Paris trace covers a 17.97 km x 10.32 km highly urban region with strongly interconnected roadways across the entire area and a more uniform geographic distribution of charge-points and distributed commuter traffic pattern. EVs in these scenarios primarily acquire energy opportunistically as they go about their normal routing however if they anticipate low availability and imminent depletion EVs will actively seek out an infrastructure charge-point to resupply from. These public infrastructure charge-points are included per current real-world deployments [27]. The number of included infrastructure charge-points is in-line with current trends in the vehicle-to-refuelling-index (VRI) for EVs [28]. In addition to consumer EVs and static charge-points, higher energy capacity electric buses from multiple service operators are also included as energy distributors in each scenario and follow their real-world routes in each city [32]. The commuting EVs are considered prosumers, with buses and charge-points representing mobile energy distributors and suppliers respectively [29].

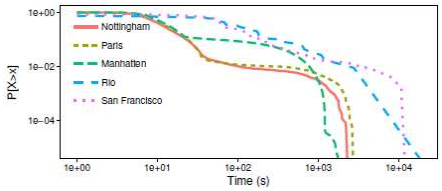

Fig. 4. Distribution of contact duration for each trace.

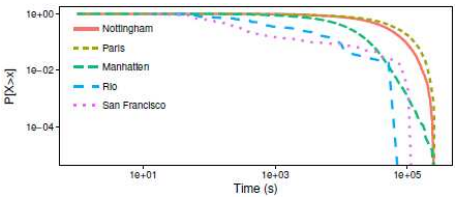

Fig. 5. Distribution of inter-contact duration for each trace.

Although Figs. 4, 5 show both the Nottingham and Paris traces are highly similar from a mobility and universal network connectivity perspective, we include both due to the substantial difference in availability of energy in each scenario. Nottingham has very few public access static charge-points compared to Paris which has seen extensive EV infrastructure development [27]. As observed previously [14], a fewer number of charge-points increases the wait times for access to grid energy supply. Likewise, Paris has a higher ratio of buses to vehicles than Nottingham meaning consumers in our SMG scenario have increased opportunity for energy acquisition from in-network distributors.

The Rio de Janeiro mobility trace follows the real-world movement of buses [30]. Similarly, for San Francisco we use an existing mobility trace of taxicabs [25] over an area of 10 km x 16 km. For each trace a sample of 100 vehicles is selected over a period of 5 days. We select suitable positions for infrastructure charge-points based on frequent points of vehicle congregation. We additionally consider a synthetic SMG scenario using an artificial Manhattan grid model with consumer EVs and limited charge points.

The described traces for Nottingham, Paris, Rio de Janeiro and San Francisco are highly social with ego-networks in each displaying distributions characteristics of scale-free networks associated with human and vehicular mobility. Whilst these traces are divergent across density and energy availability criteria, we believe it is important to also consider a scenario in which nodes are only marginally socially linked in order to explore the effectiveness of CONCEDE when social ties are significantly weaker. Though the Manhattan grid scenario displays social connectivity properties (Figs. 4, 5), all EVs have ego-networks which are large and show uniform encounter frequency distribution, i.e. each node has an ego-network which contains many contacts but there is no significant strength between a social tie to one node versus to any other.

Figs. 6, 7, 8, 9, 10 show the number of critically depleted nodes over time in each scenario. CONCEDE successfully detects and minimises the impact of attack in all cases. CONCEDE identified and excluded the malicious nodes in each trace with only a 10% increase in the number of low charge EVs.

ISBN 978-3-903176-13-3

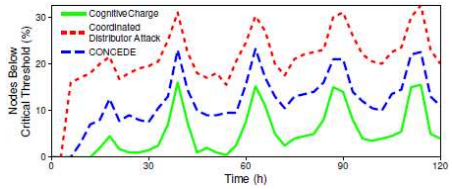

Fig. 6. Average percentage of vehicles with critically low battery levels in the Nottingham scenario.

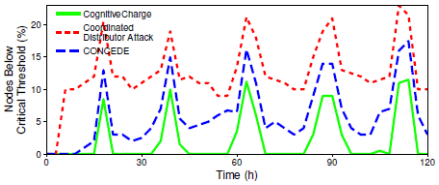

Fig. 7. Average percentage of vehicles with critically low battery levels in the Paris scenario.

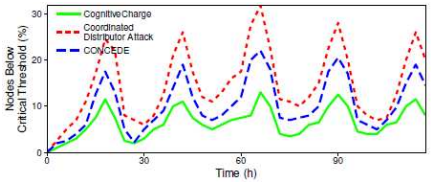

Fig. 8. Average percentage of vehicles with critically low battery levels in the San Francisco scenario.

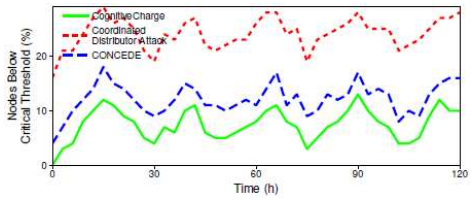

Fig. 9. Average percentage of vehicles with critically low battery levels in the Rio de Janeiro scenario.

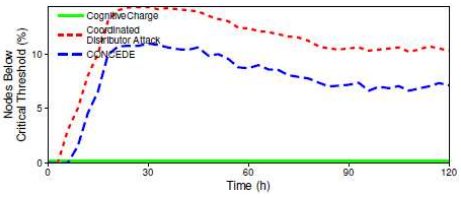

Fig. 10. Average percentage of vehicles with critically low battery levels in the Manhattan scenario.

The depletion levels in the Manhattan scenario Fig. 10 show a slight reduction in attack impact and improvement in recovery which is the result of the robustness inherent to CognitiveCharge. Energy is moved to the region experiencing depletion. CONCEDE improves this further through its dishonest behaviour identification mechanism which reduces the overall attack impact. Despite this, due to the sustained nature of the attack, pure CognitiveCharge cannot fully recover to the baseline levels of depletion.

We observe that CONCEDE adapts to the attack, improving the availability amongst the most vulnerable targeted nodes and network regions. In our experiments the attack is not only severe due to the malicious information propagation leading to targeted community depletion but also as a result of the loss of the providers as in-network mobile supply points. As such, even with CONCEDE present we do not see a complete return to baseline levels because the loss of these nodes as additional energy transporters and suppliers reduces overall energy availability.

In Figs. 6, 7, 8, 9 clear delineations can be observed between days due to the influence of time of day on energy expenditure and ability to charge. In each of these scenarios some nodes were able to access static grid infrastructure overnight which directly reduced the number of severely depleted nodes through the morning as saturated nodes could supply those in need and without local resources. Despite increased availability from infrastructure in the Paris scenario the results observed are similar to those for Nottingham (Figs. 7, 6). The additional static charge-points, whilst reducing overall depletion levels, do not help directly mitigate the attack because their observed information requires physical ferrying by mobile nodes to other network regions. The Rio de Janeiro SMG scenario Fig. 9 shows most significant attack impact on critical depletion levels due to the sparsity of the topology limiting charge availability. Long intervals between contact time with surplus energy carrying EVs and charge points increase the vulnerability of nodes and thus the severity of the attack.

Beyond depletion levels we can see that CONCEDE reduces the impact of the attack on the time a critically depleted node must wait until it can access a suitable energy supply opportunity. Due to limited space we show representative examples for the pseudo-realistic Nottingham real-world San Francisco traces in Fig. 11 and Fig. 12. When under attack nodes must wait substantially longer to receive charge – over 1 hour in the Nottingham scenario whereas in the baseline scenario this can be as low as 10 minutes. The San Francisco scenario shows similar results with a threefold increase in wait time over the baseline scenario. In all instances CONCEDE reduces the wait time for energy access from available nodes with surplus charge.

We also performed experiments to better understand what the rate of failure of the CONCEDE detection of malicious prosumers is. Our early results showed that there is a learning curve of the nodes that accurately detect the malicious nodes and are able to avoid them (failure detection rate drops from 15% to 5% of undiscovered malicious prosumers over 5 days). We have calculated failed detection rates as average per day across all nodes that are highly likely to meet all the malicious nodes.

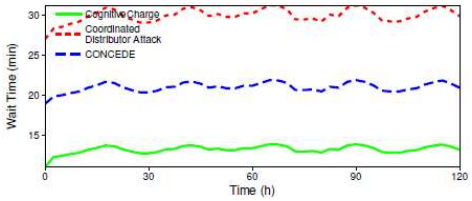

Fig. 11. Wait time duration in the San Francisco scenario until energy acquisition for nodes in need.

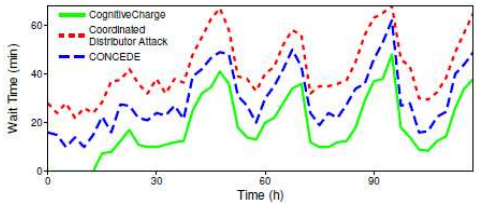

Fig. 12. Wait time duration in the Nottingham scenario until energy acquisition for nodes in need.

VI. Conclusion

In this paper we proposed CONCEDE, a robust, cross-layer integrity awareness, threat detection, and attack mitigation scheme which integrates seamlessly into CognitiveCharge [14], our existing approach for adaptive, delay-tolerant energy exchange in dynamic SMGs. CONCEDE enhances the robustness of CognitiveCharge nodes with the ability to more rapidly collaboratively respond to threat of energy depletion from malfunctioning or actively malicious nodes. With CONCEDE, identified dishonest nodes can be avoided for energy exchange until their perceived integrity is restored, thus protecting both individuals, communities and regions from energy depletion attack and malfunction resulting in incorrect information propagation.

We evaluated CONCEDE using a diverse range of real-world and pseudo-realistic heterogeneous SMG traces from Europe, North America, and South America. CONCEDE nodes successfully detected and mitigated the severity of depletion amongst nodes in a community under a sustained energy depletion attack across multiple criteria. In our future research we seek to address the wider impact of our work on the defined users, exploring effective measures for managing the dynamic trade-offs between secure, predictive localised energy exchange and stakeholder privacy requirements in complex mobile SMG environments.

References

[1] Milena Radenkovic, Andrew Grundy, Efficient and adaptive congestion control for heterogeneous delay-tolerant networks, Ad Hoc Networks, Volume 10, Issue 7, 2012, Pages 1322-1345

[2] D. B. Richardson, “Electric vehicles and the electric grid: A review of modeling approaches, impacts, and renewable energy integration” Renewable and Sustainable Energy Reviews, vol.19, 2013.

[3] M. Ponce-Jara, E. Ruiz, R. Gil, E. Sancrist´obal, C. P´erez-Molina, and M. Castro, “Smart grid: Assessment of the past and present in developed and developing countries,” Energy Strategy Reviews, vol. 18, pp. 38–52, 2017.

[4] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, “Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies,” IEEE Transactions on Industrial Informatics, 2018.

[5] G. Sorebo, Smart grid security : An end-to-end view of security in the new electrical grid. Boca Raton, FL: CRC Press, 2012.

[6] M. H. Rehmani, F. Akhtar, A. Davy, and B. Jennings, “Achieving resilience in sdn-based smart grid: A multi-armed bandit approach,” in 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), 2018, pp. 366–371.

[7] D. Sperling, “Electric vehicles: Approaching the tipping point,” Bulletin of the Atomic Scientists, vol. 74, no. 1, pp. 11–18, 2018.

[8] M. J. Kass, “The end of the road for gas-powered automobiles?” Natural Resources & Environment, vol. 32, no. 4, pp. 53–54, 2018.

[9] edie, “Mission Possible: Achieving a Sustainable Future.” International Telecommunication Union, May-2018.

[10] S. Saha, A. Lukyanenko, and A. Yl¨a-J¨a¨aski, “Cooperative caching through routing control in information-centric networks,” in 2013 Proceedings IEEE INFOCOM, 2013, pp. 100–104.

[11] D. Bertsimas, V. F. Farias, and N. Trichakis, “The price of fairness,” Operations Research, vol. 59, no. 1, pp. 17–31, 2011.

[12] T. Lomax, S. Turner, and R. Margiotta, “Monitoring urban roadways in 2000: Using archived operations data for reliability and mobility measurement.” Texas Transportation Institute; https://static.tti.tamu.edu/tti.tamu.edu/documents/FHWA-OP-02-029.pdf, 2001.

[13] M. Zhong, P. Lingras, and S. Sharma, “Estimation of missing traffic counts using factor, genetic, neural, and regression techniques,” Transportation Research Part C: Emerging Technologies, vol. 12, no. 2, pp. 139–166, 2004.

[14] M. Radenkovic and A. Walker, “CognitiveCharge: Disconnection tolerant adaptive collaborative and predictive vehicular charging,” in Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, 2018

[15] C. Binding et al., “Electric vehicle fleet integration in the danish edison project - a virtual power plant on the island of bornholm,” in IEEE PES General Meeting, 2010, pp. 1–8.

[16] R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, et al, “Peer to peer energy trading with electric vehicles,” IEEE Intelligent Transportation Systems Magazine, vol. 8, no. 3, pp. 33–44, 2016.

[17] B. Roberts, K. Akkaya, E. Bulut, and M. Kisacikoglu, “An authentication framework for electric vehicle-to-electric vehicle charging applications,” in 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2017, pp. 565–569.

[18] M. Radenkovic and I. Vaghi, “Adaptive user anonymity for mobile opportunistic networks,” in Proceedings of the Seventh ACM International Workshop on Challenged Networks, 2012, pp. 79–82.

[19] M. Radenkovic, A. Benslimane, and D. McAuley, “Reputation aware obfuscation for mobile opportunistic networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 1, Jan. 2015.

[20] S. Zakhary, M. Radenkovic, and A. Benslimane, “Efficient location privacy-aware forwarding in opportunistic mobile networks,” IEEE Transactions on Vehicular Technology, vol. 63, no. 2, Feb. 2014.

[21] R. Zhang, X. Cheng, and L. Yang, “Flexible energy management protocol for cooperative ev-to-ev charging,” in 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6.

[22] M. Wang, M. Ismail, R. Zhang, et al, “Spatio-temporal coordinated v2v energy swapping strategy for mobile pevs,” IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1566–1579, May 2018.

[23] S. Trifunovic and A. Hossmann-Picu, “Stalk and lie-the cost of sybil attacks in opportunistic networks,” Computer Communications, vol. 73, no. PA, pp. 66–79, Jan. 2016.

[24] E. M. Daly and M. Haahr, “Social network analysis for information flow in disconnected delay-tolerant manets,” IEEE Transactions on Mobile Computing, vol. 8, no. 5, pp. 606–621, May 2009.

[25] M. Piorkowski, N. Sarafijanovic-Djukic, and M. Grossglauser, “CRAWDAD dataset epfl/mobility (v. 2009-02-24).” Downloaded from https://crawdad.org/epfl/mobility/20090224, Feb-2009.

[26] M. Radenkovic, A. Walker, and L. Bai, “Towards better understanding the challenges of reliable and trust-aware critical communications in the aftermath of disaster,” in The 14th International Wireless Communications and Mobile Computing Conference (IWCMC 2018), 2018.

[27] Open Charge Map, “The global public registry of electric vehicle charging locations.” https://openchargemap.org, 2018.

[28] T. Gnann, S. Funke, N. Jakobsson, P. Pl¨otz, F. Sprei, and A. Bennehag, “Fast charging infrastructure for electric vehicles: Today’s situation and future needs,” Transportation Research Part D: Transport and Environment, vol. 62, pp. 314–329, 2018.

[29] European Commission. “Energy, transport and environment indicators”. Luxembourg: Publications Office of the U, 2017.

[30] D. Dias and L. H. M. K. Costa, “CRAWDAD dataset coppeufrj/riobuses (v. 2018-03-19).” Downloaded from https://crawdad.org/coppe-ufrj/RioBuses/20180319, Mar-2018.

[31] Ari Keränen, Jörg Ott and Teemu Kärkkäinen: The ONE Simulator for DTN Protocol Evaluation. SIMUTools'09: 2nd International Conference on Simulation Tools and Techniques. Rome, March 2009.

[32] M. Radenkovic, A. Walker, “CognitiveCharge/CONCEDE Mobility Datasets”, http://eprints.nottingham.ac.uk/55772/8/WONS2019.zip, available from Feb 2019.