IET Cyber-Physical Systems: Theory & Applications

Case Study

Hijacking internet-connected devices to provoke harmful oscillations in an electrical network: a feasibility assessment

ISSN 2398-3396
Received on 11th February 2019
Revised 16th September 2019
Accepted on 10th February 2020
doi: 10.1049/iet-cps.2019.0012
www.ietdl.org

Hugh Gowing[1], *Paul Cuffe*[1] ✉

[1]*School of Electrical and Electronic Engineering, University College Dublin, Dublin 123609, Ireland*

✉ *E-mail: paul.cuffe@ucd.ie*

Abstract: Internet-connected devices will represent an increasing proportion of the load served by electric power systems. As these devices could conceivably be hijacked and controlled remotely by a malicious actor, they could represent a new threat vector against the dynamic security of a power system. Such attack strategies have not been considered in the existing literature on power system cybersecurity. As an initial scoping exercise, the present case study explores whether such devices could be remotely hijacked and then maliciously power-cycled at particular frequencies to deliberately provoke harmful oscillations in an electrical grid. To gauge the broad feasibility of this novel style of attack, dynamic simulations are performed on two representative test power systems, at differing levels of attacker and defender resources. These simulations show that power-cycling just 1% of consumer loads at a system's resonant frequency may sometimes provoke harmful electromechanical oscillations throughout a national grid. This novel simulation exercise, therefore, implies that cybersecurity vulnerabilities at the consumer side could jeopardise the physical integrity of a nation's entire electricity supply.

1 Introduction

The synchronised cadence of pedestrians' footsteps can sometimes induce harmful structural oscillations on a bridge [1]: could a malicious actor exploit similar dynamics to attack a power system? To the authors' best knowledge, this question has not been addressed in the extant research literature. This issue is growing in importance, as an increasing proportion of end-consumer devices integrate internet of things (IoT) functionality [2], which means these electrical devices could potentially be hijacked by a malicious cyberattacker. While the idea of interfering with consumer-scale electronic equipment to harm a nation-spanning grid may seem implausible, there are reasons to believe that this is a credible attack vector. A national grid is fundamentally an electromechanical system and thereby exhibits resonant frequencies where oscillations may be undamped and liable to grow to dangerous extremes [3]. The present work seeks to scope the broad viability of such an attack, which has not been addressed in the extant literature on power system cybersecurity [4].

The research questions for the present case study are: is it possible to provoke harmful oscillations in a power grid by remotely switching a set of geographically dispersed loads on-and-off at some specific frequency? What proportion of the total system load would need to be hijacked to make this style of attack feasible? To what extent can system defences, in the form of power system stabilisers (PSS), mitigate this type of destabilising attack? (A PSS is fitted to a synchronous generator's excitation system, and damps oscillations that may develop between the rotor angles of different machines [5]).

The specifics of how IoT devices could be hijacked, or how their power-cycling could be synchronously modulated across a wide area, are not treated in the present work. Likewise, optimising such forced oscillation attack strategies, or their corresponding defences are beyond the narrow scope of this feasibility assessment. The present case study is largely qualitative in character, seeking to address the broad feasibility of such an attack strategy: the quantitative simulations performed in pursuit of this are necessarily somewhat notional.

Recent reviews [4, 6–8] of the existing literature on power system cybersecurity indicate that forced oscillation attacks have not been widely studied. Work such as [9] shows that unintentional cyclic load fluctuations can cause unwanted resonance in a power system, and such resonances have historically been implicated in large-scale system outages [10]. Likewise, work in [11] found that a power injection of just 10 MW, modulated on-and-off at a carefully chosen frequency by a malicious generator, could provoke powerflow fluctuations of up to 477 MW on certain lines, potentially causing tripping and cascading failure. Such work is of increasing importance as distributed generation continues to displace conventional synchronous plant and is thereby taking an increasing role in maintaining grid stability [12, 13]

Work in [14] explored the malicious manipulation of dynamic prices signals to invoke a particular response from smart loads, and concluded: 'cyberattacks in a local community are able to impact a larger area power grid.'

There are established examples of real world cyberattacks against power systems: for instance, the 2015 incident in Ukraine [15] was the first blackout widely-accepted to be caused by such means. While this intrusion required a highly skilled group of hackers working for six months to infiltrate a well-defended central control system, the attack vector proposed in the present work exploits vulnerabilities in consumer-owned IoT devices, where cybersecurity is much weaker. Work in [16] explains that IoT-enabled devices have difficulties meeting stringent security protocols and [2] sounds a pessimistic note: 'Most connected devices are secured with a factory-supplied default username and password. Users rarely change these.' Lax security such as this at the consumer side would become worrisome indeed if it opens a vector for entire power systems to be attacked.

Section 2 describes two simulation methodologies, one which shows how an attacker can observe a system's resonant frequency, and another that estimates the potential severity of an attack targeting such an oscillatory mode, using two well-known power systems as a case study. These test cases and results are presented in Section 3, and Section 4 concludes.

2 Methodology

To facilitate an initial feasibility assessment, this section outlines one potential strategy that a cyberattacker could use to identify and exploit resonant modes in a power system using only publicly observable information. This attack strategy is presented in a proof-of-concept form for scoping purposes. This section also describes a test procedure, where dynamic simulations of a realistic power system are performed to gauge the impact of the novel attack strategy. With these validation simulations, it is possible to identify the portion of a system's total load that an intruder would need to hijack to allow a harmful attack to be mounted.

The validation simulations are intended to give a broad indication of the feasibility of forced oscillation cyberattacks: where assumptions are made they favour the attacker. For this reason, the methodology is pessimistic. The specifics of how devices might be remotely hijacked, or how their power modulations could be synchronised, are outside the scope of the present methodology.

2.1 Attacker's strategy

While sophisticated analysis techniques can identify the resonant oscillatory modes in a power system [17], this study assumes that a cyberattacker would have neither the expertise nor the requisite data to apply these. Instead, a simple perturb-and-observe approach is proposed, which treats the power system as a ‘black-box’, as follows:

- The cyberattacker installs two phasor measurement units in the system, separated by some suitable electrical distance [18]. Affordable, open-source units are available [19], and these can be plugged-in at domestic voltage levels [20] to provide observability of phase angle differences between geographical areas.
- The cyberattacker takes control of just a small percentage of the IoT loads in the power system and uses these as an excitation ‘probe’ e.g. $\text{payload}_{\text{test}} = 1\%$.
- These probing loads are switched off-and-on for a short period, slowly sweeping through a suitable frequency range, $\text{freq}_{\text{test}}$ of 0.1→2.0 Hz to cover the likely inter-area resonant modes.
- Using telemetered data, the cyberattacker can observe which excitation frequency causes the largest separation in voltage angles between the two remote phasor measurement units. This frequency, freq_{res}, can be interpreted as being a highly resonant mode of the system, and will not be heavily dependent on the specific locations of the phasor measurement units.

With this resonant frequency, freq_{res}, identified, the cyberattacker then commits their full portfolio of hijacked consumer loads to maliciously force oscillations at this frequency. This perturb-and-observe strategy gives an up-to-date snapshot of a system's most resonant oscillatory mode under the prevailing powerflow and generator dispatch conditions. Notably, the availability of low voltage phasor measurement units now means that a system's dynamic characteristics can be observed by any network user.

2.1.1 Load composition selection: It may be assumed that a cyberattacker would target the hijacking of the load type (constant power, current or impedance) that would be most effective at provoking oscillations. To account for this, simple simulations were run as follows to identify the most attractive load type to hijack: first, 1% of the load across selected load buses was used as a probe, and these were modulated at a particular test frequency. Several simulations were run, changing only the load composition of these probing loads. The load composition causing the biggest deviation in system stress indicators was selected, and then used for both the perturb-and-observe simulations and the ensuing forced oscillation attack itself.

2.2 Attack efficacy appraisal simulations

Dynamic electromechanical simulations of power systems experiencing the described attack strategy are undertaken to answer the following questions:

- Can widespread resonance be excited by forced modulation of dispersed loads?
- What portion of the system load, $\text{payload}_{\text{attack}}$, needs to be hijacked in order to excite damaging resonances?
- How effective are PSS defences at nullifying this style of attack?

2.2.1 Measuring attack severity: The primary metric that is used to identify a successful attack is the presence of sustained growing oscillations in any of the system stress indicators, as this implies that some generators will eventually become de-synchronised, damaged or tripped off by protection measures. The system stress indicators were defined as rotor angle separations between generators in different areas, generator terminal voltages, and generator rotor speeds. An attack was deemed to be successful if growing oscillations could be provoked in any of these indicators, even if the magnitude of these was inconsequential over the simulated timeframe. However, there is also a case where the oscillations are very large but do not grow; thus a secondary set of threshold-breaking conditions were also proposed to judge the efficacy of an attack, as follows:

- Any generator terminal voltage consistently exceeding 1.05 p.u. or falling below 0.95 p.u. [21].
- Any generator rotor speed operating continuously over 1.01 p.u. or below 0.99 p.u. [22].
- The absolute value of rotor angle separation between generators in different areas exceeding 90°.

Each system is attacked with an increasing portfolio of hijacked loads, $\text{payload}_{\text{attack}}$, until one of these metrics is satisfied or until a 15% load hijacking requirement is reached.

2.3 Summary of the attack simulation algorithm

As shown in Fig. 1, the present methodology embodies two distinct phases. In the first phase, perturb-and-observe, the simulations are performed from the attacker's perspective, to illustrate how even modest observability of a system (just two pmus), and modest controllability (merely $\text{payload}_{\text{test}} = 1\%$) can allow a resonant frequency, freq_{res}, to be inferred. Proceeding then to the appraise attack efficacy phase, simulations are then performed from the system's operators perspective, to determine how much hijacked load controllability, $\text{payload}_{\text{attack}}$, an attacker would need for the forced oscillation attack to be successful at harming the network.

3 Results

3.1 Test platform

Simulations of the different attack scenarios were conducted in the Simscape package for Simulink [23], which facilitates the dynamic modelling of the electrical and mechanical components that make up a synchronous power system. Two standard power systems, Kundur and Quebec, were selected as test beds to gauge the feasibility of the proposed attack strategy. These systems were selected as they are widely-known and pre-existing validated dynamic models for them are publicly available.

To promote transparency, replication, and reanalysis of the present results, the underlying scripts, test system data, and supplementary documentation have been placed on a persistent open access repository [24].

3.1.1 Kundur system: The first test system is a version of Kundur's two-area, four-machine system [25], as shown in Fig. 2. The Kundur system has generators 1 and 2 and a single 1027 MVA load in area 1, with two 220 km tie-lines connecting it to area 2, which is made up of generators 3 and 4 and a 1820 MVA load. Initially, 413 MW is exported from area 1 to area 2. All generators are of the round-rotor type and are identical except for their inertia coefficients.

Three types of PSS are included in this model, based on frequency, speed, and accelerating power, and each of these types has a validated tuning for this system. The escalation of this system's defences, as per the procedure of Section 2.2.2, is described in Table 1. The attacker was assumed to have controllability of a portion of each of the four spot loads in the system, and the hijacked components were modelled as constant power loads.

3.1.2 Quebec system: The second test system is a version of Quebec's power system for which a dynamic model is available [26], as shown in Fig. 3. This is a larger and more complex network, with 29 buses serving a total load of 21.5 GVA. It contains seven generators in four different areas that are connected to each other by long tie-lines, thereby suggesting the presence of inter-area modes. All generators are of the salient-pole type.

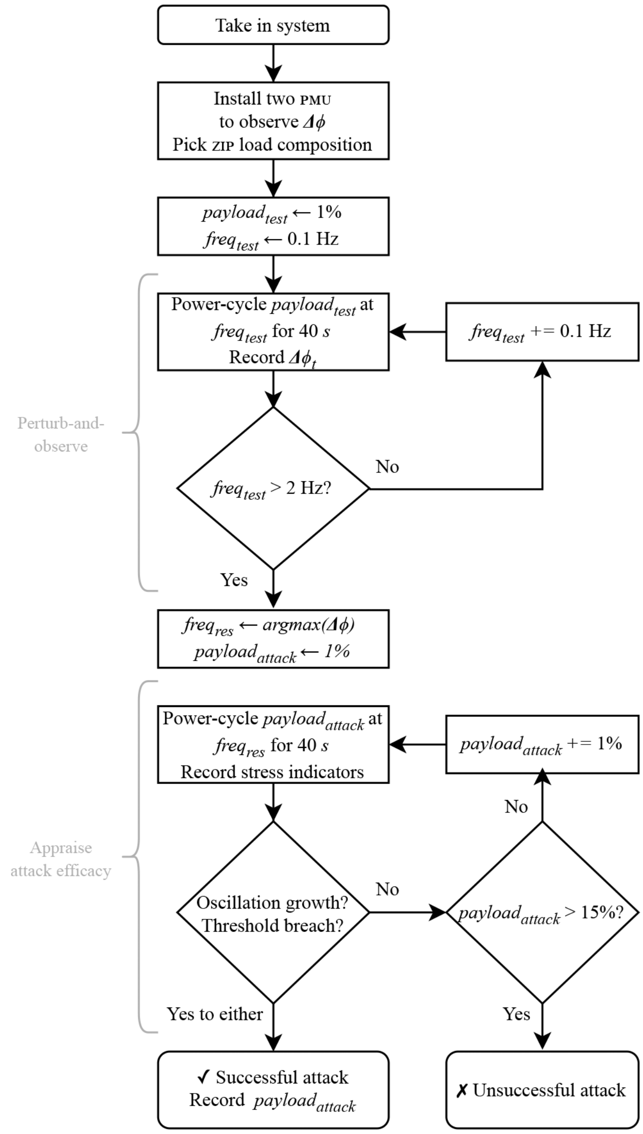
Take in system
Install two PMU to observe $\Delta\phi$ Pick ZIP load composition
$payload_{test} \leftarrow 1\%$
$freq_{test} \leftarrow 0.1$ Hz
Power-cycle $payload_{test}$ at $freq_{test}$ for 40 s Record $\Delta\phi_t$
$freq_{test}$ += 0.1 Hz
$freq_{test} > 2$ Hz?
No
Yes
Perturb-and-observe
$freq_{res} \leftarrow argmax(\Delta\phi)$
$payload_{attack} \leftarrow 1\%$
Power-cycle $payload_{attack}$ at $freq_{res}$ for 40 s Record stress indicators
$payload_{attack}$ += 1%
Appraise attack efficacy
Oscillation growth? Threshold breach?
No
$payload_{attack} > 15\%$?
No
Yes to either
Yes
✓ Successful attack Record $payload_{attack}$
✗ Unsuccessful attack

Fig. 1 *Flowchart representation of the attack simulation methodology*

Two types of default PSS were implemented, accelerating power and frequency based, taking default tunings from [23]. The attacker was assumed to have controllability over a portion of the 11 constant power spot loads in the system: the remaining 17 constant impedance loads were unaffected. The escalation of this system's defences, as per the procedure of Section 2.2.2, is described in Table 2.

3.1.3 Escalation of system defences: Electrical networks have protections against undamped oscillations, in the form of PSS units, which will be fitted to some subset of the generators in the network. To estimate how effective these may be at damping forced oscillations, each test system is simulated with various levels of PSS defences. To represent a gradual escalation in system defence capability, each network was incrementally equipped with the PSS whose location and type provided the smallest increase in damping ability. This represents a pessimistic upgrade path and this assumption will favour the attacker. The procedure for augmenting the two test systems with various levels of PSS defences is as follows:

- At each incremental level of system defence, one additional generator was equipped with a PSS.
- The most resonant frequency of the system at each level of protection was determined as per Section 2.1. The PSS type and location that allowed the largest oscillations at this frequency was determined, and this was chosen as the incremental PSS to be added to the system's protections. This provides a lower bound on a system's resilience at a particular PSS penetration level. [The least-protective location for the incremental PSS was found by placing it in turn at each available unprotected generator and observing the worst inter-area power flows: the least-protective type was determined by simulating each style of PSS control [5] at that location and observing the largest resulting oscillations in the system stress indicators.]

3.2 Attack simulation results

3.2.1 Mode identification results: The procedure of Section 2.1 was applied to each test system, at each level of PSS protection, to demonstrate how an attacker could use the simple perturb-and-observe approach to infer the resonant mode for each of these networks. The resonant frequencies found in this way are shown in the rightmost columns of Tables 1 and 2.

Each system was then attacked, at each level of its defence escalation, by targeting the resonant modes shown in Tables 1 and 2. The attack started by power-cycling just 1% of the system's total load as a probe, per section 2.1. With each system's most resonant frequency thereby identified, the attack payload was increased in steps of 1% until a successful attack was evident or until a load capture requirement of 15% was reached, i.e. a far greater portion of the system load than IoT devices could reasonably represent. Each attack was sustained for 40 s.

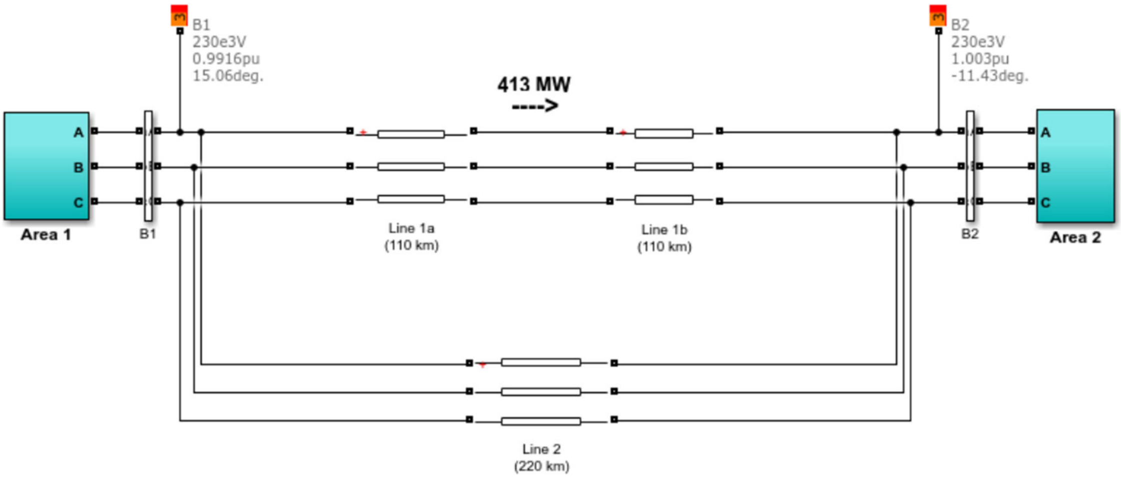

Fig. 2 *Kundur dynamic test system, as implemented in Simscape [23]*

Table 1 Kundur system: escalation of PSS defences

Installed PSS count	Incremental PSS type	Incremental PSS location	Resonant frequency, Hz
none	—	—	0.50
1	speed	gen. 2	0.55
2	speed	gen. 1	0.55
3	speed	gen. 3	0.55
4	accel. power	gen. 4	0.30

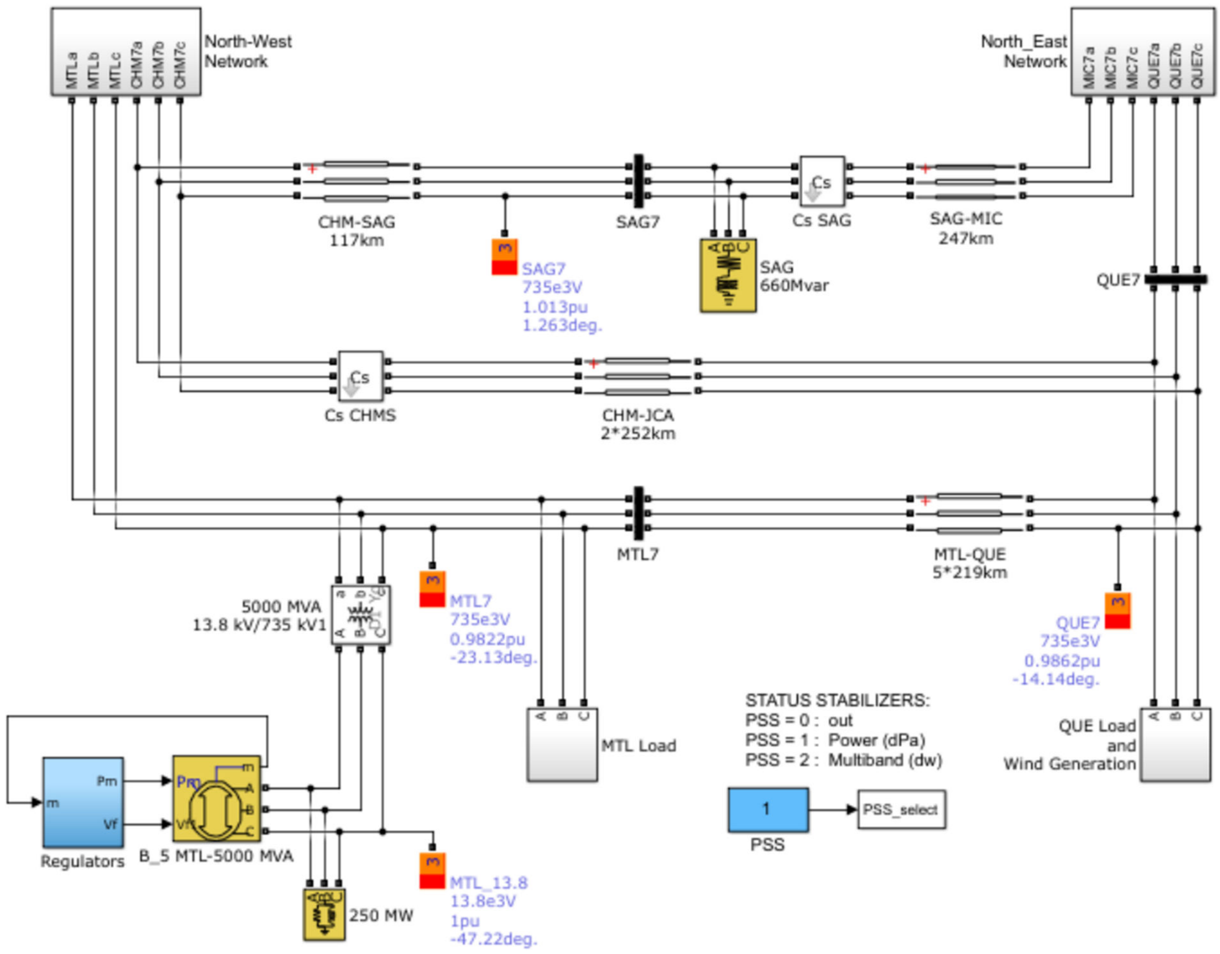

Fig. 3 *Quebec 29 bus dynamic test system, as implemented in Simscape [23]*

Table 2 Quebec system: escalation of PSS defences

Installed PSS count	Incremental PSS type	Incremental PSS location	Resonant frequency, Hz
none	—	—	1.0
1	accel. power	gen. 5	1.0
2	accel. power	gen. 3	1.0
3	accel. power	gen. 6	1.0
4	accel. power	gen. 1	1.0
5	accel. power	gen. 4	1.0
6	accel. power	gen. 7	1.0
7	accel. power	gen. 2	1.0

3.2.2 Resiliency of Kundur system: When protective measures are not in place, hijacking just 1% of this system's load is sufficient to provoke growing oscillations in the system stress indicators. For instance, Fig. 4 shows that rotor speeds accelerate rapidly to dangerous levels (>1.01 p.u.) within just the first 20 s of the attack. As shown in Table 3, the same load capture requirement of just 1% can damage the system even when two PSS are in place: however, above this level of protection, even attacking with 15% load hijacking is inadequate to meaningfully disturb the system.

3.2.3 Resiliency of Quebec system: As illustrated in Table 4, this system is also quite susceptible to a forced oscillation attack. Worryingly, at every level of system defences, a threshold breach can be provoked in at least one of the system stress indicators: the terminal voltage of generator 5 is particularly vulnerable in this respect. When equipped with up to two PSS, control of just 1% of the system load can invoke oscillations that both grow in extent and breach thresholds for the system stress indicators. The addition of a third PSS stabilises the system somewhat, but even at and above this level of protection, an attack with 8% of system load is sufficient to provoke thresholds breaches for some of the system stress indicators. For instance, rotor speeds oscillations for the unprotected system are shown in Fig. 5: while these are modest in amplitude, the sustained growth of this system stress indicator is worrisome.

3.2.4 Comparison of system resilience: It is clear from Tables 3 and 4 that the Quebec system is substantially less resilient against forced oscillation attacks as compared to the Kundur system. Relevantly, inter-area oscillations typically arise when sets of generators are separated from each other by long, electrically weak tie-lines, as the restoring torques diminish with electrical distance. The Quebec system is much larger and more complex than the Kundur system: notably, its NW and NE generating areas are separated from each other by a single 364 km tie-line, whereas the

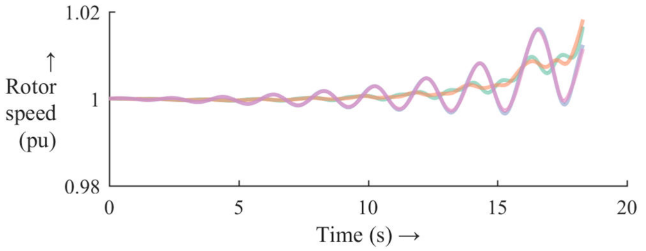

Fig. 4 *Growing and threshold-breaking oscillations in rotor speeds when the unprotected Kundur system is attacked at 0.5 Hz: each of the four traces shows the rotor speed of a specific generator*

Table 3 Kundur system: load capture requirements

Installed PSS count	Growing oscillations provoked?	Damaging thresholds breached?	Load capture requirement
none	yes	yes	1%
1	yes	yes	1%
2	yes	yes	1%
3	no	No	—
4	no	no	—

Table 4 Quebec system: load capture requirements

Installed PSS count	Growing oscillations provoked?	Damaging thresholds breached?	Load capture requirement, %
none	yes	yes	1
1	yes	yes	1
2	yes	yes	1
3	no	yes	8
4	no	yes	8
5	no	yes	8
6	no	yes	8
7	no	yes	8

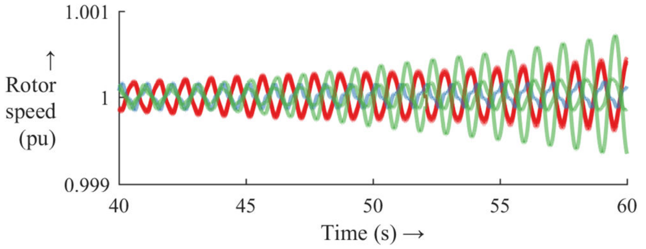

Fig. 5 *Growing, but modest, oscillations in rotor speeds when the unprotected Quebec system is attacked at 1.0 Hz with 1% of the system load*

generating areas in the Kundur system were connected by two parallel 220 km tie-lines, and this strong electrical connection contributes to its resilience.

This comparison implies that realistic, nation-scale national grids may be more susceptible to a forced resonance attack, as compared to small, simple test platforms such as the Kundur system.

3.2.5 Results context and realism: It is important to note that the simulations were inherently pessimistic, as it was generously assumed the attacker could synchronously modulate loads of the optimally damaging composition across a wide network, while the escalation of system defences was according to incremental additions of the least-effective PSS types and locations.

4 Conclusions

The present work explored the broad feasibility of a novel attack strategy against electrical networks, whereby remotely hijacking consumer IoT loads and power-cycling them at a system's resonant frequency could provoke electromechanical oscillations. A simple perturb-and-observe method for detecting such resonant frequencies was proposed. Dynamic simulations were then undertaken to qualitatively scope the broad feasibility of such an attack strategy, at various levels of attacker and defender resources. These tentative quantitative results indicate that forced oscillation attacks against power systems may indeed be feasible. For instance, on both test systems, it was possible to damage the network by hijacking just 1% of the load. However, the test simulations also indicated that networks that have widespread deployments of generator PSS units are much less susceptible to induced instability. On the Kundur system, installing two PSS units allowed the system to fully withstand the forced oscillations attack. On the Quebec system, installing three PSS units was sufficient to prevent the provocation of growing oscillations, although hijacking 8% of system loads were still sufficient to cause threshold breaches at this level of system defences. Further work is necessary to articulate how damaging this novel attack strategy could be against more realistic electrical networks, to explore how this may best be defended against, and to ascertain the robustness of these results to different parameters values and modelling decisions.

5 Acknowledgments

This work has emanated from research conducted with the financial support of Science Foundation Ireland under the sfi Strategic Partnership Programme Grant Number sfi/15/spp/e3125. The opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Science Foundation Ireland.

6 References

[1] Strogatz, S.H., Abrams, D.M., McRobie, A., *et al.*: 'Theoretical mechanics: crowd synchrony on the millennium bridge', *Nature*, 2005, **438**, (7064), p. 43

[2] Corcoran, P.: 'The internet of things: why now, and what's next?', *IEEE Consum. Electron. Mag.*, 2016, **5**, (1), pp. 63–68

[3] IEEE Power & Energy Society.: 'Identification of electromechanical modes in power systems', Available at. http://sites.ieee.org/pes-resource-center/files/2013/11/TR15_Modal_Ident_TF_Report.pdf

[4] He, H., Yan, J.: 'Cyber-physical attacks and defences in the smart grid: a survey', *IET Cyber-Phys. Syst., Theory Appl.*, 2016, **1**, (1), pp. 13–27

[5] Larsen, E.V., Swann, D.A.: 'Applying power system stabilizers part I: general concepts', *IEEE Trans Power Appar Syst*, 1981, **PAS-100**, (6), pp. 3017–3024

[6] Li, Z., Shahidehpour, M., Aminifar, F.: 'Cybersecurity in distributed power systems', *Proc. IEEE*, 2017, **105**, (7), pp. 1367–1388

[7] Rasmussen, T.B., Yang, G., Nielsen, A.H., *et al.*: 'A review of cyber-physical energy system security assessment'. 12th IEEE Power and Energy Society PowerTech Conf. IEEE, Manchester, UK, 2017

[8] Arghandeh, R., von Meier, A., Mehrmanesh, L., *et al.*: 'On the definition of cyber-physical resilience in power systems', *Renew. Sustain. Energy Rev.*, 2016, **58**, pp. 1060–1069

[9] Rao, K.R., Jenkins, L.: 'Studies on power systems that are subjected to cyclic loads', *IEEE Trans. Power Syst.*, 1988, **3**, (1), pp. 31–37

[10] Kosterev, D.N., Taylor, C.W., Mittelstadt, W.A.: 'Model validation for the August 10, 1996 WSCC system outage', *IEEE Trans. Power Syst.*, 1999, **14**, (3), pp. 967–979

[11] Sarmadi, S.A.N., Venkatasubramanian, V.: 'Inter-area resonance in power systems from forced oscillations', *IEEE Trans. Power Syst.*, 2016, **31**, (1), pp. 378–386

[12] Hernández, J.C., Bueno, P.G., Sanchez Sutil, F.: 'Enhanced utility-scale photo-voltaic units with frequency support functions and dynamic grid support for transmission systems', *IET Renew. Power Gener.*, 2017, **11**, (3), pp. 361–372

[13] Bueno, P.G., Hernández, J.C., Ruiz Rodriguez, F.J.: 'Stability assessment for transmission systems with large utility-scale photovoltaic units', *IET Renew. Power Gener.*, 2016, **10**, (5), pp. 584–597

[14] Liu, Y., Hu, S., Zomaya, A.Y.: 'The hierarchical smart home cyberattack detection considering power overloading and frequency disturbance', *IEEE Trans. Ind. Inf.*, 2016, **12**, (5), pp. 1973–1983

[15] Liang, G., Weller, S.R., Zhao, J., *et al.*: 'The 2015 Ukraine blackout: implications for false data injection attacks', *IEEE Trans. Power Syst.*, 2017, **32**, (4), pp. 3317–3318

[16] Yang, Y., Wu, L., Yin, G., *et al.*: 'A survey on security and privacy issues in internet-of-things', *IEEE Internet Things J*, 2017, **4**, (5), pp. 1250–1258

[17] Rogers, G.: 'Demystifying power system oscillations', *IEEE Comput. Appl. Power*, 1996, **9**, (3), pp. 30–35

[18] Cuffe, P., Keane, A.: 'Visualizing the electrical structure of power systems', *IEEE Syst. J.*, 2017, **11**, (3), pp. 1810–1821

[19] Laverty, D.M., Best, R.J., Brogan, P., *et al.*: 'The openPMU platform for open-source phasor measurements', *IEEE Trans. Instrum. Meas.*, 2013, **62**, (4), pp. 701–709

[20] Liu, Y., Zhan, L., Zhang, Y., *et al.*: 'Wide-area-measurement system development at the distribution level: an FNET/GridEye example', *IEEE Trans. Power Deliv.*, 2016, **31**, (2), pp. 721–731

[21] 'IEEE guide for AC generator protection', IEEE Std C37102-2006 (Revision of IEEE Std C37102-1995), 2006, pp. 1–177

[22] IEEE.: 'Generator protection: fundamentals and application', Available at. http://www.ewh.ieee.org/r6/san_francisco/pes/pes_pdf/Gen_Protection.pdf

[23] The Mathworks Inc.: 'Simscape', Available at. https://uk.mathworks.com/products/simscape.html

[24] Cuffe, P.: 'Raw data, scripts and dissertation related to 'hijacking internet-of-things devices to provoke harmful oscillations in an electrical network', Available at. https://figshare.com/s/207f485f7a94df1d722d

[25] The Mathworks Inc.: 'Performance of three PSS for interarea oscillations', Available at. https://uk.mathworks.com/help/physmod/sps/examples/performance-of-three-pss-for-interarea-oscillations.html

[26] The Mathworks Inc.: 'Initializing a 29-bus, 7-power plant network', Available at. http://tinyurl.com/yd6e2bpq