Received: 5 June 2020 | Revised: 23 November 2020 | Accepted: 23 December 2020 | IET Cyber-Physical Systems: Theory & Applications

DOI: 10.1049/cps2.12002

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH PAPER

Enhanced cyber-physical security using attack-resistant cyber nodes and event-triggered moving target defence

Martin Higgins[1] | **Keith Mayes**[2] | **Fei Teng**[1]

[1]Department of Electrical and Electronic Engineering, Imperial College London, Exibition Road, South Kensington, London, UK

[2]Royal Holloway, University of London, Information Security Group, Egham, London, UK

Correspondence

Fei Teng, 1113, Imperial College, Electrical Engineering Building, South Kensington Campus Exhibition Rd, South Kensington, SW7 2BU, London.
Email: f.teng@imperial.ac.uk

Funding information

ESRC under Grant, Grant/Award Number: ES/T000112/1; Centre for Doctoral Training in Power Networks, Grant/Award Number: EP/L015471/1

Abstract

A cyber-physical authentication strategy to protect power system infrastructure against false data injection (FDI) attacks is outlined. The authors demonstrate that it is feasible to use small, low-cost, yet highly attack-resistant security chips as measurement nodes, enhanced with an event-triggered moving target defence (MTD), to offer effective cyber-physical security. At the cyber layer, the proposed solution is based on the MULTOS Trust-Anchor chip, using an authenticated encryption protocol, offering cryptographically protected and chained reports at up to 12/s. The availability of the Trust-Anchors allows the grid controller to delegate aspects of passive anomaly detection, supporting local as well as central alarms. In this context, a distributed event-triggered MTD protocol is implemented at the physical layer to complement cyber side enhancement. This protocol applies a distributed anomaly detection scheme based on Holt-Winters seasonal forecasting in combination with MTD implemented via inductance perturbation. The scheme is shown to be effective at preventing or detecting a wide range of attacks against power system measurement system.

1 | INTRODUCTION

The power system is arguably the most critical of all modern networked infrastructures. To some extent, water, communications, sanitation and defence systems are dependent on a stable electricity supply and it is no wonder that the power system has become a key target for hackers seeking to disrupt or destroy. In 2015, Ukraine experienced one of the first successful (and well documented) cyber attacks against a distribution power grid with the consequence that around 300,000 people were disconnected from their power supply [1]. This attack brought significant focus to the area of cyber attacks against power systems. However, to some extent, the impact of the Ukraine attacks was limited as the attackers chose a non-stealthy method of implementing the attack. If the attackers had opted for a stealthy attack type, such as false data injection (FDI) attacks, they may have been able to continue attacking and achieve much greater damage.

In the past, the majority of works focussed on either physical or cyber security enhancements in isolation, however, more recently, works have been published which demonstrate the importance of considering overlapping cyber and physical solutions [2]. A practical and affordable system design that protects against attacks at both physical and cyber layers and allows for distributed protection is proposed and evaluated.

The cyber domain of a power system is susceptible to various attacks. National guidelines suggest the use of cryptographic tools for authentication and encryption [3]. However, as outlined in [4], supervisory control and data acquisition (SCADA) networks (which are used for monitoring and controlling power systems), often lack secure modern encryption. This can be due to the age of assets (encryption and security of networks being a more recent concern) or requirements for high speed in data processing with encryption adding too much of a time delay in measurement transmission [5]. The size and scale of power networks can also make the cost of refitting prohibitive, with increased focus put on 'sweating' assets rather than incorporating new infrastructure. As a result, while a new cyber layer protection solution is urgently required, it must be low cost (to ensure practical take up), secure by the Common Criteria security framework [6] and also shown not to impede data transmission.

Furthermore, the links between cyber and physical systems are also vulnerable to the attacks. In the case of the power measurement system, a simple alternative to attacking the

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2021 The Authors. *IET Cyber-Physical Systems: Theory & Applications* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

cyber-secured measurement node is to modify the analogue (or physical) measurement source, which cannot be protected by cyber domain solutions. The attackers may conduct FDI attacks by manipulating analogue measurements before they reach the cyber-secured point.

One attack type that uses this form of measurement changing is the FDI attack. FDI attacks use system information to remain hidden while attacking systems measurement to misguide the WLS-based state estimation [7]. Although extensive research have been conducted to detect FDI attacks, the vast majority of papers operate on the assumption of residual testing based on centralised state estimation (CSE) [8]. The consequences of a successful FDI attack can be severe. For example, in [9] it is shown that FDI attacks can be used to promote load shedding via the system operator or overload certain lines and in [10] it was shown how FDI attacks can be used to mask transmission outages. A few papers recently started to tackle FDI attacks from a distributed perspective. In [11–13] FDI attacks against distributed Kalman style or extended Kalman style filtering are explored to show how dynamic style estimation (at the individual state or measurement) can still have potential susceptibilities to attack.

1.1 | Moving target defence against FDI attacks

Moving target defence (MTD) is the process of introducing controlled changes into an underlying system in order to increase the difficulty for adversaries in attacking a system.

1.1.1 | Cyber system MTD

Within the cyber domain, MTD has primarily been applied at the communications layer for information or networked security. As shown in [14], cyber-based MTD strategies tend to operate around specific asset uses of servers and network channels. For example, a defender may designate certain channels or servers as unavailable during certain times and if an adversary in the course of their attack attempts to use them they will be exposed. There are also MTD applications in cryptography wherein MTD can increase the security of the system by having dynamic keys [15]. Packet drops are another fairly common consideration for cyber-based MTD. Packet drops are used in [16], where the loss in packet information and the consequent impact on the control system were used to evaluate FDI attacks on control sensors. Packet drops are also considered for the SCADA system MTD in [17]. In general, MTD at the cyber layer is performed via a change of communication protocol or asset utilisation, and is typically lower cost.

1.1.2 | Physical system MTD

By contrast, physical layer MTD usually involves altering the system outright. The most commonly suggested form of MTD in the physical system is topology-driven MTD. These topology changes are usually implemented through transmission switching [18] or more commonly by admittance perturbation via distributed flexible AC transmission system (D-FACTS) devices [19–22]. These contrast quite directly with most cyber forms of MTD which usually contain static topologies. Very few papers have explored transmission switching as a legitimate method of applying MTD in the power system. This is because, while in theory it could be effective at driving increased residuals in the case of an attacker unaware of MTD as shown in [23], the impacts of such an approach on power system control and cost to operation would be undesirable. Also, from the attacker's perspective, identifying these changes and countering are much easier in the case of transmission switching. By comparison, D-FACTS-based applications are much more common and cause less overall impact to power system stability and have lower operational costs. Indeed, while it has been shown that MTD can be effective, limited work has been carried out into how it should be implemented in power systems. Questions around the frequency and when MTD should be applied remain. Continuous application of MTD will result in significantly higher costs [24] and time-based application, that is once per hour, is possible but will risk attacks slipping between applications (sometimes called in-cycle attacks). The authors argue that MTD should only be applied if there is a creditable suspicion that the system is under attack. In [25], an event-driven MTD is proposed for control systems and the authors adopt a similar idea for power system application.

1.2 | Contributions

A practical and affordable system design is proposed and designed that protects against both physical and cyber layer attacks and allows for distributed protection. The authors demonstrate how a cyber-physical authentication process can provide a foundation for system security at every level of measurement and transmission. This process is illustrated in Figure 1.

1.2.1 | Cyber layer

In the cyber layer, we propose creating trustworthy measurement nodes by using a small pay load, encrypted protocol to secure the measurement reporting system while maintaining the required frequency of reporting. Each node is based on a highly tamper-resistant security chip that performs measurement capture, processing and reporting. The chip acts as a trustworthy platform, supporting the secure communication protocol with the grid authority (GA). The combination of the chip and protocol offers effective protection against implementation attacks and communications attacks, such as man-in-the-middle/FDI. The secured platform also allows confident delegation of some limited processing to the nodes, such as the proposed anomaly check and MTD triggering.

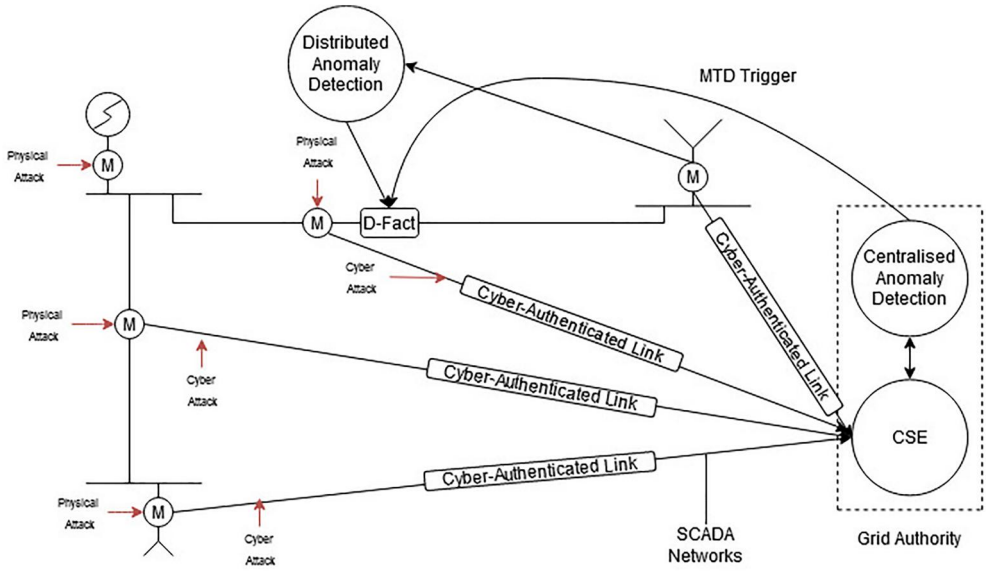


FIGURE 1 Outline of a proposed cyber-physical defence model featuring the moving target defence trigger mechanism, metering and distributed anomaly detection

The MULTOS Trust-Anchor for secure measurement transmission and MTD delegation has not been applied previously. This may be because MULTOS platforms have been traditionally in the form of secured smart card and passport chips, which do not have general external I/O. Although authenticated encryption has been standardised for some time, it has only relatively recently been studied on such security chips. The design secures the logical and implementation security of the system, but importantly, it provides a framework for delegated/distributed implementation of trusted functions and self-defensive mechanisms. We have also shown that the secure nodes can sample, process and locally react, much faster than would be feasible for a centralised system, offering the potential for new algorithms and research.

1.2.2 | Physical layer

In the physical layer, the authors propose a protection protocol based on event-triggered MTD. The protocol consists of an initial anomaly detection followed by MTD and traditional CSE. The anomaly detection uses Holt-Winters seasonal forecasting distributed to the individual measurement. The seasonality captures the intra-day demand differences to minimise the overall window for attack. If the anomaly detection is triggered, MTD is then implemented via inductance perturbation of D-FACTS devices. This changes the system model and drive detection of the FDI attack via increased residual errors. The event trigger comes prior to the application of MTD and is based on distributed measurements to target and minimise the overall use of MTD. This is important as the FDI attacks are stealthy from a centralised residual detection perspective, but their impacts can still be seen in the distributed changes to power flows. One of the key motivation drivers for this research is that MTD can be expensive to implement given the sub-optimal use of assets from an optimal power flow perspective, as shown in [26]. Very few works have addressed the importance of distributed measurement with respect to FDI attacks and none that the authors have seen combine a distributed and centralised approach as has been done here.

Section 2 provides background to the proposed approaches. This includes outlining the state estimation environment for the power system. Section 3 proposes and describes a secure solution based on an authenticated encryption (AE) protocol and the use of distributed security chips (SC). A novel event-triggered MTD is proposed in Section 4 and the Holt-Winters seasonal forecasting technique as triggering strategy is outlined. Experiments, performance results and the effectiveness of security measures are discussed in Section 5, with conclusions and suggestions for future work in Section 6.

2 | BACKGROUND

2.1 | Cyber vulnerability of SCADA system in power system

An attacker has several options when seeking to undermine the measurement and reporting system. The node itself can be attacked to either ensure that the node does not perform as intended or to reveal a credential (such as a cryptographic key) or proprietary functionality. It is also possible that the measurement source (e.g. value to be sampled) could be modified so that incorrect values are captured, but then securely delivered to the GA (upstream physical attack). However, the node's remote communications link presents the most attractive

target, and attackers may seek to remove, modify or replay valid transmissions, or generate fake transmissions that might be accepted by the node, and inject consequently false data into the state-estimator downstream of the physical system.

2.1.1 | Node implementation attacks

Critical infrastructure may be attacked in a variety of ways. Adhering to information security best practice for the functional design of a measurement node (e.g. for algorithms, protocols, processes and keys) is not sufficient, as attacks may target the implementation.

Logical security attacks target weak design typically in the algorithms, keys and poor software either within the node platform, the measurement application or the loading and configuration functionality. Physical attacks generally require considerable expertise, equipment and time. For example, an attempt may involve decapsulating a chip, hardware reverse engineering, probing buses and memories and modifying tracks. Fault attacks are less intrusive, they disrupt normal operation of the chip, but without damage. For example, faults can be generated by voltage glitches or radiation pulses. Under fault conditions, an unprotected chip may reveal sensitive information, for example RSA keys [27]. Side-channel leakage is the leakage of sensitive information via an unintended channel. This can be key- or data-dependent timing, variations in power consumption or electromagnetic emissions. Simple analysis techniques (see [28,29]) are powerful against naive implementations. In the case of a power measurement system, a simple alternative to attacking the measurement node is to modify the analogue measurement source (physical attack). A similar effect is achieved by manipulating any part of the path that digitises and communicates the source measurement value, up until the point when it is within the node.

All of the these attacks can be successful against implementations that do not have specialist security protection. However, there is much industry expertise for the protection of secured micro-controller chips, which is exploited in this proposal, as discussed in Section 3.

2.1.2 | Adversary threat model

The authors make the assumption of a well resourced attacker, similar to those seen in [1], capable of launching attacks in both the cyber and physical realms. The attacker can attack either remotely via SCADA networks or directly at the physical sensor locations themselves. It is also assumed that the attacker has the capability to structure an FDI attack via the changing of meter measurements so that it stealthy. Consistent with this is the assumption that the attacker has knowledge of the original system topology of the power system, but is not aware of MTD configurations. An outline of the respective cyber and physical attack types follows.

2.1.3 | Node communication attacks

To undermine communications between two legitimate parties, an attacker may attempt to:

1. Passively eavesdrop
2. Send a new message assuming a legitimate identity
3. Delay, replay, or re-order legitimate messages
4. Modify a legitimate message
5. Block some legitimate messages
6. Denial of service (DoS) transmissions

The goal of eavesdropping is to capture unprotected data or information that can reveal credentials, such as keys or counters, which aid attacks against the protection. For grid measurement transmission, the primarily concern is the integrity of measurements, rather than confidentiality, however encrypting messages also protects associated control data and provides an extra barrier to attackers. Depending on the communications channel, an attacker might simply be able to source a fake message, or may have to be positioned as a "man-in-the-middle". In either case, the attack will be defeated by mutual authentication of communicating parties, as the attacker will not have the cryptographic credentials to authenticate, or to fake, or modify a valid message. Most communications systems experience some variation in transmission delay, but, excessive delay (or replay) can be detected by timestamps. Message re-ordering can also be detected by chaining encrypted transmission sequences. If in normal operation a system occasionally loses messages, then an attacker could block some without being detected, however limited data loss could be overcome by redundant transmissions. DoS would prevent legitimate messages getting through, however it is a condition detectable by the legitimate communicating parties, which should be able to take some alarm and/or remedial action.

2.2 | False data injection attacks on state estimation

In terms of the physical attack target, a power grid state estimation system subject to FDI type attacks is considered [30]. FDI attacks focus on misleading system operators by introducing false information within the distributed grid system measurements, to damage the physical grid, or its operation, or cause financial consequences. From the attacker's perspective, a major advantage of the FDI attack is that it may be performed stealthily; meaning that if the false data is structured to seem plausible it will appear like a system under normal conditions to the operator. While the majority of early works focussed on a linear approximation of the FDI attack, it was shown in [31] that an AC attack model was indeed possible, provided the attacker had knowledge of the system topology. A comprehensive review of FDI attacks can be found in [8]. The basis

for CSE and FDI attacks is outlined here. Under CSE, a set of n state variables $\mathbf{x} \in \mathbb{R}^{n\times 1}$ estimated by analysing a set of m meter measurements $\mathbf{z} \in \mathbb{R}^{m\times 1}$ with a corresponding error vector $\mathbf{e} \in \mathbb{R}^{m\times 1}$ is considered. The non-linear vector function $\mathbf{h}(.)$ relating meter measurements $\mathbf{z}$ to states $\mathbf{h}(\mathbf{x}) = (h_1(\mathbf{x}), h_2(\mathbf{x}), \ldots, h_m(\mathbf{x}))^T$ is shown by

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}. \tag{1}$$

Active and reactive power flow measurements under the non-linear expression are defined by

$$P_{ij} = V_i^2 g_{ij} - V_i V_j g_{ij} \cos\Delta\theta_{ij} - V_i V_j b_{ij} \sin\Delta\theta_{ij}, \tag{2}$$

$$\begin{aligned} Q_{ij} = &- V_i^2 (b_{ij} + b_{ij}^{sh}) + V_i V_j g_{ij} \cos\Delta\theta_{ij} \\ &- V_i V_j b_{ij} \sin\Delta\theta_{ij}. \end{aligned} \tag{3}$$

While the linear model is no doubt easier, it contains a number of assumptions around voltage angle and other areas [32]. Under certain circumstances, a linear model can be used for operation due to its close approximation. These assumptions are:

1. Line resistances are considered negligible compared to line reactance, that is $R_L \ll X_L$
2. The voltage profile is flat and voltage amplitude equivalent across all nodes
3. The voltage angle differences are small, which results in linearisation of the sine/cosine elements in power flow equations

Under these assumptions $V_i \approx V_j$, the small angle differences result in $\sin\Delta\theta_{ij} \approx \theta_{ij}$ and g_{ji} is much smaller than b_{ji}, leading to the linear approximation for power flow

$$P_{ij} = -b_{ij}\theta_{ij}. \tag{4}$$

which gives the linear approximation as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}. \tag{5}$$

The state estimation problem is to find the best fit estimate of $\widehat{\mathbf{x}}$ corresponding to the measured power flow values of $\mathbf{z}$. Under the most widely used estimation approach, the state variables are determined by minimisation of a WLS optimisation problem as

$$\min J(\mathbf{x}) = (\mathbf{z} - \mathbf{h}(\mathbf{x}))^T \mathbf{W} (\mathbf{z} - \mathbf{h}(\mathbf{x})). \tag{6}$$

$\mathbf{W}$ is a diagonal $m \times m$ matrix consisting of the measurement weights. Under the AC model, the minimisation is done using the partial derivative with respect to the states and iterative processes.

This is done using iterative processes, usually the Newton-Raphson [7] utilising the Jacobian $\mathbf{J}$ of partial derivatives

$$\mathbf{J} = \begin{vmatrix} \frac{\delta h_1}{\delta x_1} & \cdots & \frac{\delta h_1}{\delta x_n} \\ \cdots & \cdots & \cdots \\ \frac{\delta h_1}{\delta x_m} & \cdots & \frac{\delta h_m}{\delta x_n} \end{vmatrix}.$$

The current approach in power systems operation for bad data detection (BDD) is to use the 2-norm of the measurement residual with a detection threshold η [7].

$$r = \|\mathbf{z} - \mathbf{h}(\widehat{\mathbf{x}})\|_2. \tag{7}$$

If $r_t > \eta$, BDD alarms will trigger and the system operator will discard the result. However, recent papers have shown these methods can be attacked by structuring the attack vector in terms of the system topology

$$\mathbf{z}_a = \mathbf{h}(\mathbf{x} + \mathbf{c}) \tag{8}$$

where c is a desired attack bias of length n applied to the state angles or voltage measurements.

$$r = \|\mathbf{z}_a - \mathbf{h}(\mathbf{x}\widehat{+}\mathbf{c})\|_2. \tag{9}$$

As discussed, the $\mathbf{z}_a$ vector is designed considering the state set $\mathbf{x}$ and bias $\mathbf{c}$ whilst also considering the transformation function $\mathbf{h}()$. This ensures that the residual can be designed such that it will fall within acceptable limits and ensure stealthiness.

3 | MULTOS TRUST-ANCHOR

The proposed solution requires trustworthy measurement nodes that are strongly attack resistant. Fortunately, there is a well-established, process of assessment to determine this, known as common criteria (CC) [6]. The CC evaluation is most commonly applied to security chips such as those used in bank cards, passports or hardware security modules (HSM). High levels of evaluation confirm strong resistance to all known attacks, including logical, physical, fault and side-channel. The resistance is based on specialist hardware, supported by software defensive measures. A CC evaluated SC should not be vulnerable to logic flow attacks, being compliant with security best practices for design and loading. To defend against physical attack, the CC chips will have numerous effective defences including passive/active shields (to impede probing), hardware encrypted buses and memories (to prevent data discovery), light and anomaly sensors (to detect decapsulation and faults) and scrambled circuitry (to impede reverse

engineering). For fault attack resistance, the hardware sensors detect fault insertion and prevent a response useful to the attacker. Software countermeasures provide secondary defences, for example, verifying an algorithm result before providing an output, and redundantly testing flags and loop counts. Side-channel leakage is well defended against with countermeasures that impede statistical averaging of signals, or reduce the source generation of the leakage. Attack countermeasures include power smoothing, noise insertion, randomisation of execution, timing equalisation and dual-rail logic (or dual CPUs).

MULTOS [33] chip platforms are quite common in CC evaluations, and the MULTOS [34] Trust-Anchor was selected for this proposal. MULTOS is a high-security multi-application smart card operating system (OS) that is managed by the MULTOS Consortium. MULTOS chips are found in a range of products including payment smart cards and electronic passports, achieving high levels of CC certification. The initialisation and personalisation of these products have strict security controls, meaning that only reviewed code and data from certified developers can be loaded. An introduction to MULTOS can be found in [35]. The Trust-Anchor is intended as a deployed hardware security model (HSM) for the Internet of Things (IoT) and differs from a smart card chip, in that it has added I/O capability and free-runs. Despite strong defensive capabilities, the chips lag behind the state-of-the-art in CPU performance and memory sizes, although they excel in cryptographic operations as they incorporate relatively high-speed crypto co-processor (CCoP) hardware; related performance evaluations can be found in [36–38]. The choice of SC means that physical, fault, side-channel and malware attacks can be reasonably assumed to be practically infeasible, and so the focus turns towards a protocol for securing the interaction between the SC and GA. A previous study for EMVCo [39] measured the performance of authenticated encryption (AE) [40] for future payment card processing, with MULTOS as a test platform. A number of AE modes were implemented, however for small message sizes (up to 32 bytes), Encrypt-then-MAC (ETM) [40] was the most efficient, due to the relative speeds of the CPU and CCoP. ETM is discussed next.

3.1 | Authenticated encryption

The ETM scheme (see Figure 2) is *mechanism 5* in ISO/IEC 19,772 [40], and is a conventional approach with separate encryption and MAC processes. The encryption stage uses block encryption in counter mode with key K, followed by a MAC (CBC_MAC used) computation on the cipher text using a different key (K′) to that used for encryption. The scheme has much to recommend it for securing grid communication. It provides authentication, confidentiality, integrity protection and has a counter for cryptographically chaining transmissions. If fixed-sized data is used (e.g. the optimum 32 bytes) then the counter may be predicted in the case of lost messages, avoiding the need for resynchronism, unless unavoidable.

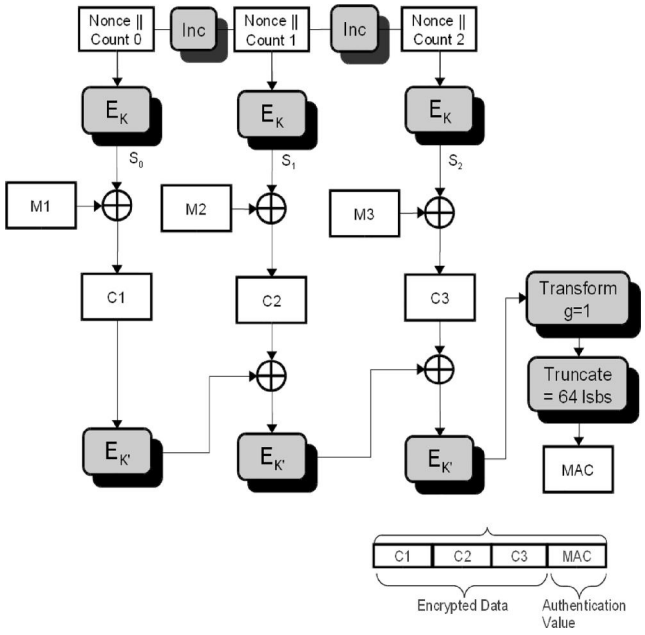


FIGURE 2 Encrypt then MAC authenticated encryption

3.2 | Node dynamic initialisation

An SC is initialised/personalised prior to use. This involves, for example, the setting (by a security authority) of IDs, long-term secret keys, access PINs, applications and data. Every node is diversified, having different keys, nonces and counters, so attacking one node provides no advantage when attacking others. As the long-term secret keys are of best-practice size and do not leave the Trust-Anchor, it is acceptable to use them in normal operations, however it is even better to use them sparingly, to create session keys, which may be refreshed as necessary. The session key establishment process also provides the opportunity to dynamically change nonce and counter values. The protocol steps for dynamic initialisation and session key generation are shown in Figure 3, with the symbols defined in Table 1.

The GA begins by generating AE session values: a random number, a random nonce and a starting counter value (random or preset). These values fill two AES blocks and are AE encrypted using the long-term secret keys and the *default* nonce and counter values for the particular Trust-Anchor. The resulting cipher blocks and MAC are then sent to the Trust-Anchor, which AE decrypts the message into two plain text blocks and computes its own version of the MAC. If the local and received MACs do not match, the protocol ends with a failure, otherwise the plain text is copied into the local copies of the random number, nonce and count, and the random number and its increment are then AES encrypted under the long-term encryption key to generate the encryption and MAC session keys, respectively. The Trust-Anchor then AE encrypts a dummy measurement report under session keys and sends to the GA (which also generates the keys). The GA AE decrypts the message using session keys, and if received and locally generated MACs match, the session key establishment has

succeeded. The received data is copied locally and the session keys are operational. The initialisation may be repeated to change the AE session keys, nonce and counter values, either as a security policy or due to lost synchronism, in which case the AE count for initialisation is reset to the default for the particular Trust-Anchor.

3.3 | Data collection processing and reporting

Referring to Figure 4 and Table 1, the Trust-Anchor is continually sampling the measurement source, storing results

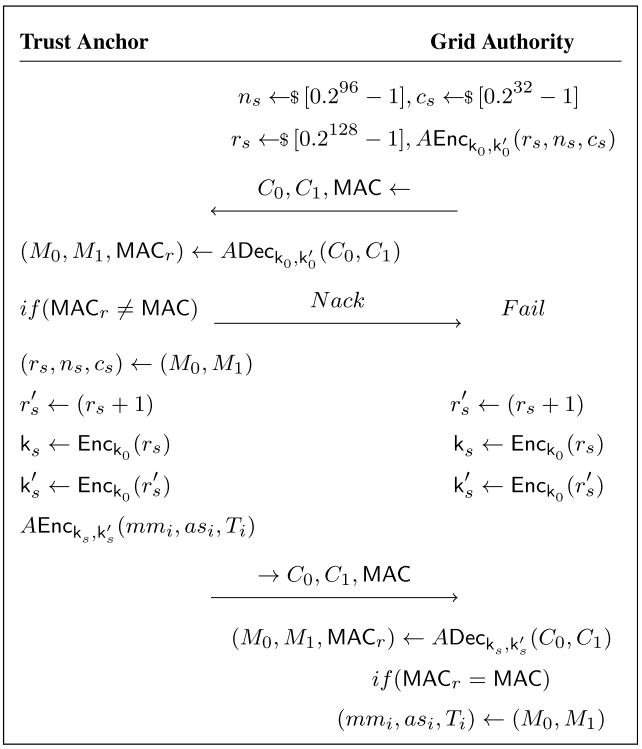


FIGURE 3 Dynamic initialisation

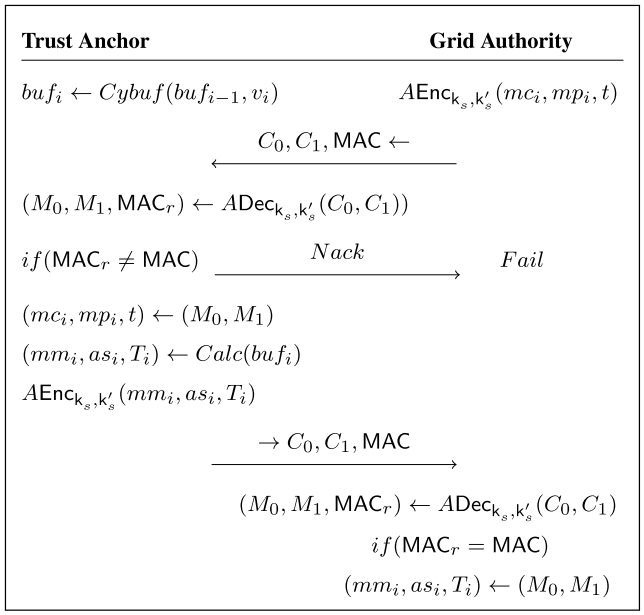


FIGURE 4 Data collection and reporting

TABLE 1 Symbol definitions

Symbol	Description
ID	Security chip ID (128-bit, or 80-bit if ICCID)
K_0, K_0'	Personalised long-term encryption and MAC keys (128-bit)
K_s, K_s'	The current session encryption and MAC keys (128-bit)
r_s, r_s'	Random values for session key generation (128-bit)
n_s	The current AE session nonce (96-bit)
c_s, c_i	Starting and i-th transmission, AE session counts (32-bit)
M_j, C_j	The j-th message and cipher blocks (128-bit)
MAC_i, MAC_r	The i-th AE token, and recomputed token (MAC: 64-bit)
t, T_i	The time and i-th Timestamp (32-bit)
as_i	The alarm status information (24-bit)
dv_i, mm_i	The i-th sample (15-bit) and model metrics (32-bit)
mp_i, mc_i	The model parameters (208-bit) and controls (16-bit)
$A\mathsf{Enc}_{\mathsf{K}_y,\mathsf{K}'_y}$	Authenticated encryption under key set y
$A\mathsf{Dec}_{\mathsf{K}_y,\mathsf{K}'_y}$	Authenticated decryption under key set y
$\mathsf{Enc}_{\mathsf{K}_y}$	AES encryption under key y

in a cyclic buffer. The GA begins a dialogue by AE encrypting under session keys, the model control fields, the model parameters and the current time. The resulting cipher blocks and MAC are sent to the Trust-Anchor, which AE decrypts the message into two plaintext blocks and computes its own version of the MAC. If the local and received MACs do not match, the protocol ends with a failure, otherwise the plain text updates local copies of model controls, parameters and real time. The Trust-Anchor then runs the detection algorithm on the buffered samples and calculates the model measurements, updates the alarm status, creates a Timestamp, generates a local alarm (if merited) and subsequently AE encrypts the results under the session keys and sends them to the GA. If the MAC verification succeeds, the report is accepted into the modelling and state estimation application. If the Trust-Anchor does not respond, or verification fails, the GA may attempt lost message recovery.

3.4 | Lost message recovery

A goal of the protocol is to tolerate the loss of at least two consecutive measurement reports, without loss of sample data. The reported model measurement field includes the latest sample plus up to seven previous samples, allowing data recovery even if blocks are lost. However, the AE counter advances during encryptions/decryptions, and using the wrong value will prevent correct decryption and MAC verification. As the message sizes are always the same, the counter value after a lost message can be estimated (within a small window), and so the GA can attempt AE decryption with several alternative counter values, and if successful will not lose any reported data. Similarly, at the Trust-Anchor, a MAC failure could indicate a missed or corrupted report request, and so the next count values could be tried for the AE decryption. In the case of irretrievable loss of synchronism, the GA will recover by using the dynamic initialisation process.

4 | EVENT-TRIGGERED MOVING TARGET DEFENCE

4.1 | Moving target defence

MTD involves using the system assets to change the underlying topology and expose FDI attacks. FDI attacks require the attack vector be structured based on the network topology. For real power residual, error at the individual measurement level will be the difference between the measured flows and estimated value from the system model such that real power residual can be expressed as a function of the individual meter measurements and system states by

$$r_{ij}^{P} = -P_{ij}^{m} + V_i^2 g_{ij} - V_i V_j g_{ij} \cos\Delta\theta_{ij} - V_i V_j b_{ij} \sin\Delta\theta_{ij}. \quad (10)$$

There is a similar equation for resultant changes in the reactive power measured residual. If the attacker is aware of the system topology, he/she can structure the attack such that the residual is small. However, if changes to the physical system are introduced (via inductance modification in this case) and the attacker does not consider this in the updated attack vector $\mathbf{z}_a$ the residual will increase as differences between the expected and injected value emerge. Where ignoring the change in voltage angles and magnitudes for a simplified view, the impact to residual will be approximated by

$$\Delta r_{ij}^{P} \approx V_i V_j \Delta b_{ij} \sin\Delta\theta_{ij} \quad (11)$$

MTD can also be enhanced to camouflage its existence to minimise the potential for attackers circumventing MTD [22,23]. However, as shown in [24], the cost of application will mean the system operator will want to minimise the overall use of MTD to only those times when the system is potentially under attack. As a result of this, we propose an MTD triggering scheme based on individual meter measurement deviations.

The proposed defensive process has three main components: the anomaly detector, the active defence protocol and the final attack verification exploiting the secured measurement and communications authentication provided by the low-cost MULTOS devices. The anomaly detection can be done either locally at the distributed level or via post processing at the same place as the CSE. For deciding the error bounds to implement the trigger the authors use Holt's exponential smoothing and forecasting and this process is outlined below.

4.2 | Anomaly detection-based triggering strategy for MTD

The authors propose a distributed trigger (located at the individual measurement level) based on Holt-Winter's Exponentially Forecasting for anomaly detection. This distributed layer of detection confers several benefits to the grid. For one, distributed error checks can be preformed much more quickly than the CSE, which can take up to a few minutes and may not even converge. Distributed measurements devices can also offer some localised control options in the case of a wider network failure of the SCADA or communications network. Crucially, with respect to FDI attacks, distributed measurement-based anomaly detection will not be susceptible to the same model-based FDI attacks outlined in [30]. Recent papers have shown that CSE can be attacked by structuring the attack vector in terms of the system topology, that is $\mathbf{z}_a = \mathbf{h}(\mathbf{x} + \mathbf{c})$ where $\mathbf{c}$ is a desired attack bias of length n. Therefore, to circumvent this type of stealthy bias injection, the authors consider a distributed error detection based on forecasted measurements to act as a trigger for MTD. The authors consider the measured vector at a given bus system as a discrete, linear model that follows the form:

$$\widehat{z}_{t+1} = F_t z_t + b_t + \nu \tag{12}$$

where $\widehat{z}_{t+1}$ is the estimated metered power flow measurements at a given time t, ν represents the system noise, which will follow a Gaussian distribution such that $\nu \hookrightarrow \mathcal{N}(0, Q)$. F_t represents the state transition factor, that is the expected change in the system state for a given time period, and b_t is the state trajectory vector used to capture long run trends and will incorporate factors such as seasonality. F_t, b_t and ν are calculated by analysing previous data trends using Holt-Winters's exponential forecasting [41] and contain seasonal elements so as to capture differences in intraday measurement resulting from load peaks. Anomaly detection in dynamic estimation will be the difference between the forecasted state value and the measured value for a given time and is given by

$$e_t = z_{t+1} - \widehat{z}_{t+1}. \tag{13}$$

The assumption is made that residuals are independent and follow a zero mean Gaussian process. They can either be defined using static pre-set limits or more commonly using an updated variance value σ^2 from observed residuals. The introduction of these additional criteria mean in order to attack stealthily (or at least not trigger MTD) the attacker would have to now satisfy both the centralised and distributed criteria such that

$$\{\mathbf{z} \in \mathbb{R}^{m\times 1} \wedge \|\mathbf{z} - \mathbf{h}(\mathbf{x})\|_2 < r_c \wedge z - \widehat{z} < r_d\} \tag{14}$$

where r_d and r_c are the alarm limits for distributed and centralised triggering/detection. It is possible that an attacker may be able to structure an attack in this manager but their flexibility in which loads can be overloaded will be greatly reduced.

4.3 | Selection of alarm limits

Alarm limits can be imposed considering a number of factors.

4.3.1 | Type-II error

Type-II error is an important consideration for alarm limits. It might be tempting to set limits artificially low to capture more potential attacks, however, this could result in higher unnecessary costs to the system operator as MTD will be triggered frequently when no attack persists. Frequent false errors can also reduce reasonable responses as the system operator grows used to seeing a high number of alarms and lacks the bandwidth to verify them efficiently.

4.3.2 | Criticality and capacity

Individual measurement criticality can also weigh into limit setting. A system operator may wish to lower limits for critical measurements. Conversely, areas with high additional transmission capacity, operating well below their thermal limits, will suffer less consequences from overloading FDI attacks. As a result, alarm limits could be relaxed to reflect the respective innate resilience of regions and focus on other weaker areas.

The authors prioritised type-II error considerations in their model and opted for limits based on the probability distribution function of a Gaussian distribution with 3 standard deviations (SD) corresponding to a 99.7% confidence interval (or type-II error of around 0.3%). This is in contrast to CSE, which usually operators with a 2 SD limit [30]. The authors believe it appropriate to have different alarm limits for these two approaches. For one, the frequency and number of distributed checks can be much higher for distributed decision making, where, unlike CSE, there are multiple potential alarm measurements, that is 34 alone in a 14-bus system, as opposed to CSE, which is only one centralised measurement. Also, as discussed, there is a cost in applying the MTD from an operational power flow perspective and it may not be desirable to use MTD triggering constantly when the branch power flow level offers no danger to the system. Ultimately, the selection of alarm limits comes down to engineering judgement. For highly critical regions, a system operator may tolerate increased false positives from a lower limit, in order to increase sensitivity.

In this model then, the upper limit is defined by $\lambda_{upper} = z_t + 3\sigma$ and lower limit $\lambda_{lower} = z_t - 3\sigma$ and they are bound such that

$$\lambda_{lower} < e_t < \lambda_{upper}. \tag{15}$$

For the power system models, an intra-day profile similar to that of a consumer load flow is assumed. This means the forecasting model needs to approximate the underlying seasonality in creating the prediction model. The Holt-Winters method is used to capture seasonality and trend when forecasting data sets. The method is made up of a forecasting equation and accompanied by three equations for the current level L_t

$$L_t = \alpha\left(\frac{z_t}{S_t}\right) + (1-\alpha)(L_{t-1} + T_{t-1}). \tag{16}$$

The overall trend of the data set T_t described by

$$T_t = \beta(L_t - L_{t-1}) + (1-\beta)T_{t-1}. \tag{17}$$

And also the seasonality component of the dataset S_t

$$S_t = \gamma\left(\frac{z_t}{L_t}\right) + (1-\gamma)S_{t-p}. \tag{18}$$

where p is the time period in a season. α, γ and β are the weighting values for level, trend and seasonality, respectively.

These are selected for a minimised RMSE error based on observing differences between the model estimates and actual values. The final predicted value using HW is described by

$$\widehat{z_t} = (L_{t-1} + T_{t-1})S_{t-p}. \quad (19)$$

4.4 | Computational considerations

It is assumed with respect to the CSE (which is already commonly used) that operators already have the capability to perform the state estimation for their system. With regard to the computation cost of applying the Holt-Winters distributed forecasting for the event trigger, the impact is small. As shown, the basic calculations are linear and can be performed quickly even with a large number of measurements. Also, as discussed, as the method is distributed to the individual meter level the computational cost of this approach is not dependent on the size of the system, that is a real impact is not expected from the curse of dimensionality resultant from system size as the core calculations and regressions remain dependent on individual measurements only.

5 | EXPERIMENTS AND FINDINGS

This section assesses the performance of the proposed detection strategy on both the standard IEEE 14-bus test system (Figure 5) and the IEEE 118-bus test system. All grid simulations were implemented using the MATPOWER toolbox in MATLAB [42] and performed using Intel Core i7-7820X CPU with 64 GB of ram running on a Windows 10 system. The node performance experiments were carried out using a MULTOS Trust-Anchor development kit.

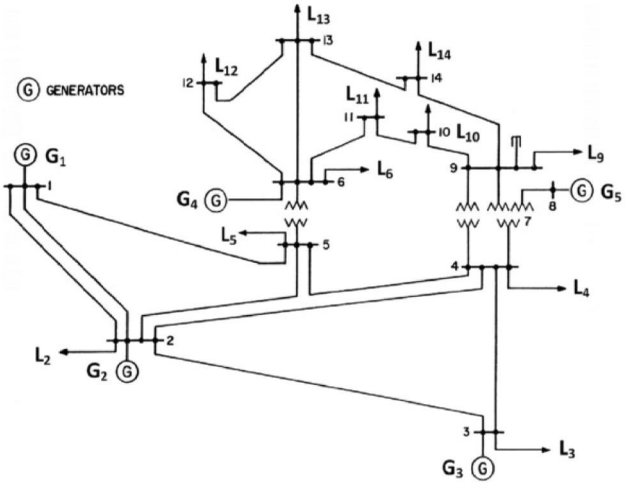


FIGURE 5 IEEE 14-bus system used for simulation

5.1 | MULTOS Trust-Anchor performance

The use of the MULTOS Trust-Anchor satisfies the node attack-resistance requirements of the proposed system, however it is a CPU speed- and memory-restricted device, and so its ability to satisfy performance requirements needs to be determined by experiment. The GA is assumed to have access to powerful server capability and so only the measurement node performance was practically investigated. The Trust-Anchor chip used for the research had digital I/O, but no analogue-to-digital converter (ADC), and so an external device was connected via its I2C bus. This did not change the attack assumptions, as it was already accepted that the analogue source value might be modified, so this was extended to the ADC chip and I2C bus. The ADC can sample orders of magnitude faster than needed, so the effective sample rate is determined by the Trust-Anchor reading from it. Normally, the Trust-Anchor would be required to free-run, but for precise experimental measurements it was run in command/response mode, where actions were triggered by commands from the GA. The Trust-Anchor was used within a breakout board that allowed PC control via a USB port. GA messages were manually created and sent to the Trust-Anchor via the MULTOS MUTIL scripting utility. MUTIL logs include message timing, and a millisecond timer was also configured within the Trust-Anchor, as a calibration check. Test software was in 'C', within a single application. For message timing precision, commands were run at least 64 times before a response, in order to compensate for residual measurement tolerance.

The initial performance results are presented in Table 2, entry row 8 is the worst case performance test. It assumes that a GA request arrives and must first be AE decrypted. The request requires the Trust-Anchor to acquire a new sample, add it to the cyclic buffer, compute the model means, test the sample and means against the model thresholds, and finally AE encrypt the resulting report for transmission back to the GA. The total execution time is 82.83 ms, supporting a maximum repetition rate of approximately 12 Hz (12/s). This suggests the Trust-Anchor could support more sophisticated,

TABLE 2 Trust-anchor results

	Function	Time (ms)	Blocks	Total (ms)	Max Rate (Hz)
1	ADC read loop	0.72	-	0.72	1391.30
2	As(1)+ update cyclic buffer	1.70	-	1.70	587.16
3	Ad(2)+ calc means	12.88	-	12.88	77.67
4	As(3)+ check thresholds	33.52	-	33.52	29.84
5	ETM decrypt	12.20	2	24.41	-
6	ETM encrypt	12.45	2	24.91	-
7					
8	Sample test and report	-	-	82.83	12.07

Abbreviations: ADC, analogue-to-digital converter; ETM, Encrypt-then-MAC.

fine-grained local processing of measurement data, as part of a distributed anomaly detection system.

5.2 | Anomaly detection

As shown in [43], the UK transmission network typical operates at around 80% capacity. Given this the authors opted to apply a 15% change in the system power flows at the attacker target. This would give the attacker enough flexibility to start to push these limits (at least at a regional level). In Figures 6 and 7 the anomaly detection algorithm implemented for a FDI attack line overload of 15% is shown. There is an initial training period for the HW seasonal forecasting for a system under normal operation. The focus is on individual line overloads and Figure 6 shows lines 1–5 for the 14-bus system for 400 h of operation with a dual peak profile occurring over 24 daily measurements. The measured data set is shown in blue and the upper and lower bounds as predicted by the Holt-winters forecast are in red. As can be seen, the first few days of implementation require a data training period with high volatility in the forecast model and high corresponding type-II error. However, this declines as the model has sufficient data to train over. Once this training period is completed, the data sets fit closely and it can be seen that no anomalies are detected over the next week of operation past the training period. A similar result can be seen for the IEEE 118-bus system in Figure 7.

In Figures 6 and 7, initially basic operation was continued for 10 days before implementing the FDI attack. This attack is stealthy from a centralised perspective but is detected by the distributed anomaly detection. This illustrates the effectiveness of the anomaly detection, which can evaluate potential FDI attacks at a distributed level (is is shown that these attacks would otherwise bypass CSE). It should be noted that there is potential for false positives with this kind of anomaly testing. As the forecasting is based on prior measurements, if new loads are added it may take a few cycles for the forecasting to reflect the new reality. However, these type-II error anomalies for the distributed detection should occur relatively rarely (0.3% of measurements in a 3 SD operating window or around 5% for a 2 SD configuration) and can be configured based on the acceptable ranges of the system operator. Furthermore, the occasional false triggering only leads to the activation of MTD to confirm the alarm, and hence the overall impact on system operation or cost is limited.

5.3 | Event-triggered MTD

In this subsection, the effectiveness of the proposed event-triggered MTD is demonstrated. The study was carried out between hours 150 and 300, as equivalent to Figures 6 and 7. The base case is first presented and it is assumed that no FDI attack is implemented. As shown in Figures 8 and 9, the residual value of BDD in CSE under normal operation is well below the alarm limit. It should be noted that while there is some initial type-II error, this is not due to the FDI attack and is, in fact, consistent with 95% chi-squared test with one anomaly point over the measurement period. In the cases where the FDI attacks are applied, a stealthy FDI attack is assumed to be launched from hour 240. In the case with only traditional BDD in CSE, Figures 10 and 11 show that the residual value does not increase tangibly over the no attack case (three type-II errors is still consistent with 2 SD confidence), which means this FDI attack is not detected. However, once the proposed protocol is applied, as shown in Figures 12 and 13, a marked increase in the overall system residual is visible, which is due to the triggered MTD, as shown in Figure 6, and the attacker's reliance on an outdated model. It should also be noted that the proposed protection protocol does not affect the centralised alarms when no attack is present, as shown between hours 240 and 300. In the case of false triggering of MTD, Figures 14 and 15 show that even though MTD is applied, there is no tangible increase in residual in the centralised alarms as the new set of measurements reflects the updated system physical topology. In this case, no false alarm for a cyber attack will be raised.

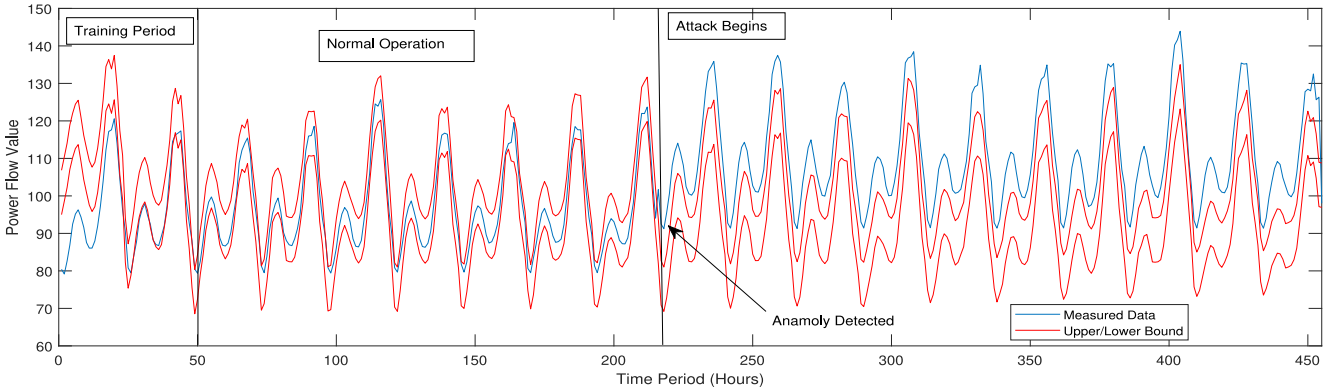


FIGURE 6 Power flow measurement across lines 1–5 in the IEEE 14-bus system over a 24-h period. System measurements shown in blue with upper/lower bounds designated via hole-winters seasonal forecasting in red. Three time periods are shown: initial training period for the forecasting, followed by under normal operation and under the initiated FDI attack

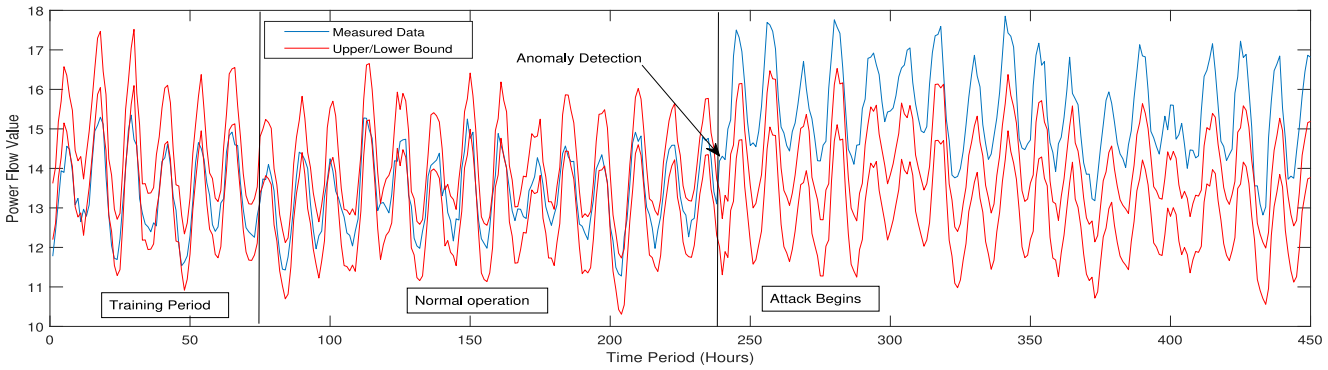


FIGURE 7 Power flow measurement across lines 1–2 in the IEEE 118-bus system over a 24-h period. System measurements shown in blue with upper/lower bounds designated via hole-winters seasonal forecasting in red. Three time periods are shown: initial training period for the forecasting, followed by under normal operation and under the initiated FDI attack

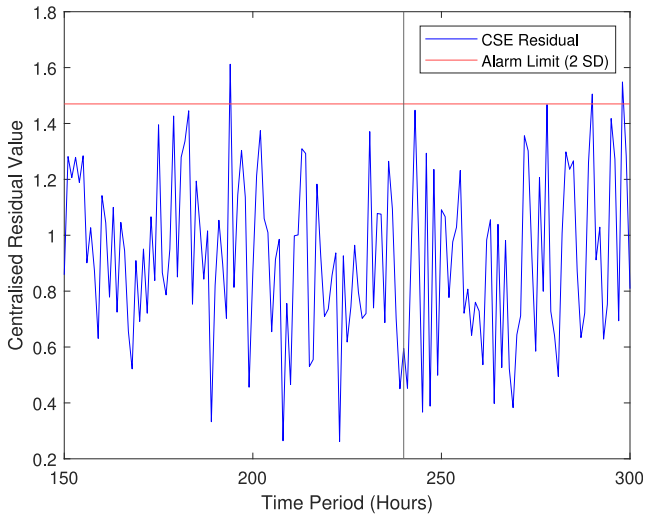


FIGURE 8 Residual value for centralised state estimation under no false data injection attack for the IEEE 14-bus system

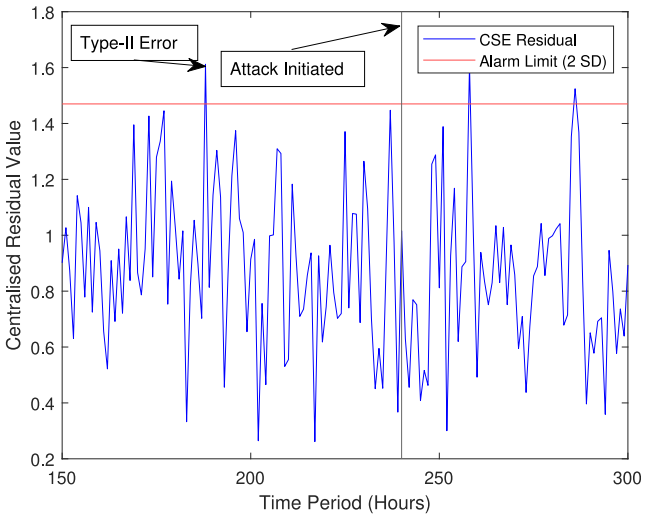


FIGURE 10 Residual value for centralised state estimation under stealthy-false data injection attack applied from 240 h without moving target defence for the IEEE 14-bus system

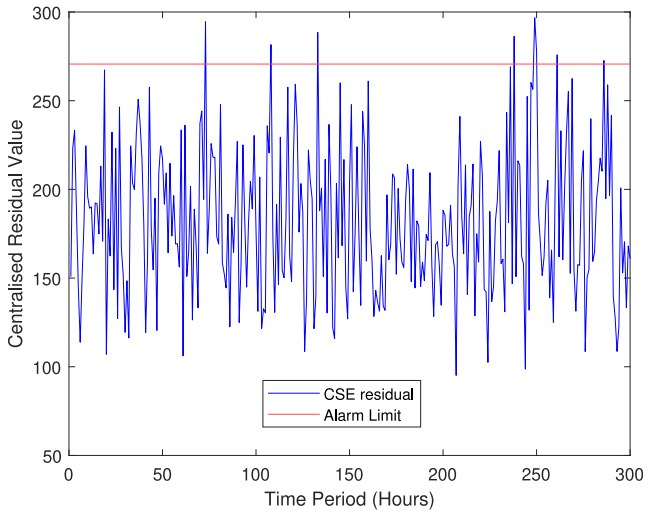


FIGURE 9 Residual value for centralised state estimation under no false data injection attack for the IEEE 118-bus system

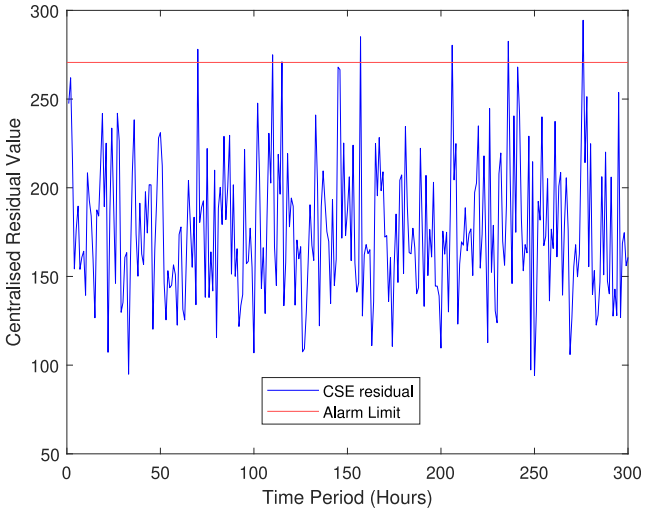


FIGURE 11 Residual value for centralised state estimation under stealthy-false data injection attack applied from 240 h without moving target defence for the IEEE 118-bus system

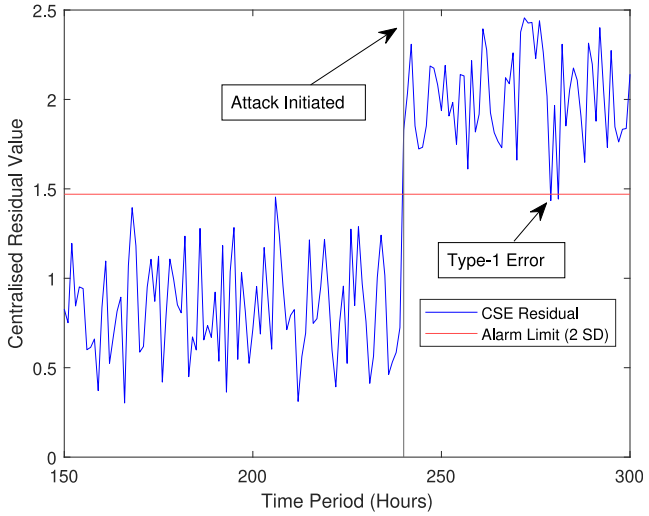


FIGURE 12 Residual value for centralised state estimation under stealthy-false data injection attack applied from 240 h with event-triggered moving target defence for the IEEE 14-bus system

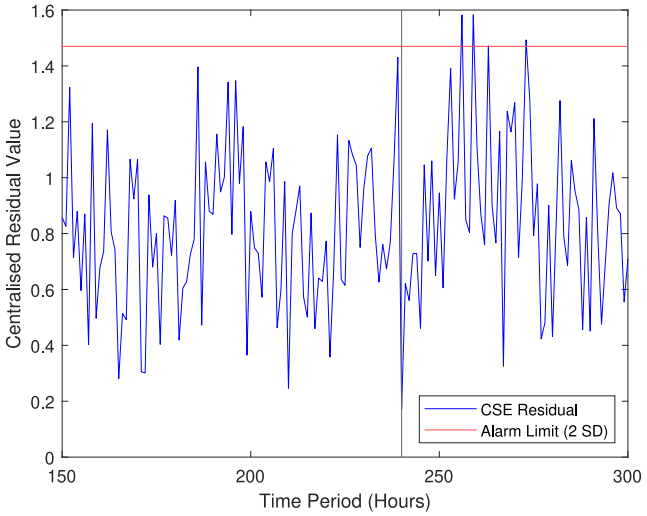


FIGURE 14 Residual value for centralised state estimation under no stealthy-false data injection attack with event-triggered moving target defence triggered at 240 h for the IEEE 14-bus system

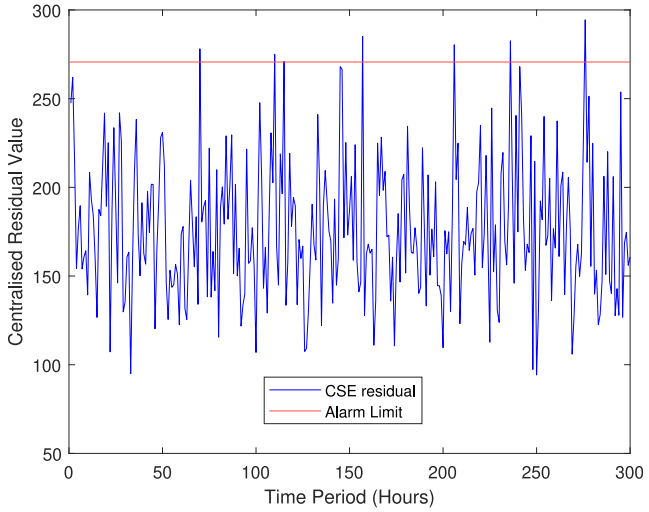


FIGURE 13 Residual value for centralised state estimation under no stealthy-false data injection attack with event-triggered moving target defence implemented at 240 h for the IEEE 118-bus system

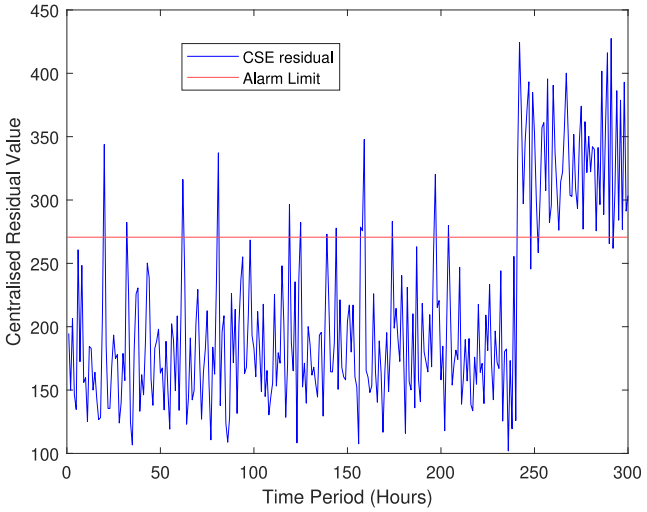


FIGURE 15 Residual value for centralised state estimation under stealthy-false data injection attack applied from 240 h with event-triggered moving target defence for the IEEE 118-bus system

5.4 | Security attack coverage

Having experimentally proven that the performance of the proposed solution is well within the design requirements, a recap on the security attack coverage is now given, as shown in Table 3. Choosing the MULTOS Trust-Anchor provides a highly attack-resistant hardware security end-point, supporting secure loading/configuration processes; making node implementation attacks practically infeasible. The use of open/standardised algorithms and diversified credentials also removes motivation for sophisticated node implementation attacks. The use of authenticated encryption prevents eavesdropping through encryption and message faking or modification via MACs. The use of a counter within the AE mode, and chaining of transmissions, prevents malicious re-ordering, and a Timestamp detects message delay. The protocol design is resilient to some lost messages (whether natural or malicious), without loss of sample data. The protocol also has resilience to loss of synchronism in counter values, and the ability to resynch when necessary, with refresh of session keys. Normal operation cannot continue under DoS attack, however the condition is detectable by the GA and nodes; and nodes are capable of raising a local alarm when denied communication to the GA. The nodes also have the capability to continue standalone passive data monitoring, to detect extreme cases of source modification. Stealthy source modification is detected by the event-triggered MTD. Malicious disablement of node local alarms can be detected by similar means.

TABLE 3 Security attack coverage

Attack Category	Cover?	How?
Node implementation attacks		
Logical/physical/fault/side channel	Yes	Inherent in Trust-anchor
Malware/personalisation/loading	Yes	Inherent in MULTOS
Node communication attacks		
Eavesdropping	Yes	AE encrypted transmissions
Fake message, legitimate ID	Yes	AE MAC will fail
Delay/replay/re-order messages	Yes	AE count chaining and Timestamp
Modify a legitimate message	Yes	AE MAC will fail
Block some legitimate messages	Yes	Protocol resilient to lost messages
DoS transmissions	Partly	Detect alarm at GA and nodes
Source modification attacks		
Overt/extreme	Yes	Detect by passive monitoring
Stealthy/subtle	Yes	Detect by MTD active tests

Abbreviations: AE, authenticated encryption; GA, grid authority; MTD, moving target defence.

6 | CONCLUSIONS

A combined cyber-physical authentication protocol for secure and reliable, state estimation of power grids, in the presence of malicious actors, has been proposed. The solution combines distributed measurement nodes based on small low-power, low-cost, security chips (SCs) via the MULTOS Trust-Anchor with a physical system event-triggered MTD protocol featuring distributed and centralised anomaly detection. Simulations were preformed on both the IEEE 14-bus and IEEE 118-bus systems to show the effectiveness of the proposed MTD and anomaly detection protocol in deriving FDI attacks. Practical experiments demonstrated that the Trust-Anchor could satisfy the most demanding GA request at a rate of 12/s; more than fast enough for envisaged operational scenarios. The communication protocol is resilient to missing measurement reports, without loss of data, and without the need for re-tries. Analysis of potential attacks showed that most were countered by the choice of Trust-Anchor and the protocol design. Passive monitoring by the node (using the delegated model) detects extreme measurement source modification. DoS will disrupt operation, but is a detectable alarm event at the nodes and the GA, and a node's passive measurement monitoring will continue under DoS attack. On top of these communications protections, the physical protection protocol looks for distributed anomalies and probes for stealthy FDI attacks using grid system assets.

6.1 | Future work

The vast majority of works in the field of FDI attacks have been based purely on simulations. Clearly, there is room for test-bed experiments for FDI attacks to observe practical examples with a view to implementation of protections into the grid. Also, on the physical side, expansion into different types of MTD protocols, that is watermarking, might also provide an interesting avenue for research. From a cyber perspective, areas such as the effect of high-rate sampling of measurement sources to detect identifying characteristics, for early warning of potential problems, or subtle attacks, invisible to current systems, would also be of interest.

ACKNOWLEDGEMENTS

This work was partly supported by an ESRC grant (ES/T000112/1) and EPSRC Centre for Doctoral Training in Future Power Networks and Smart Grids (EP/L015471/1). The authors would like to thank Chris Torr at MULTOS for his expert support and guidance, and Crisp Telecom Ltd. for access to test and development facilities.

ORCID

Fei Teng https://orcid.org/0000-0002-6828-0294

REFERENCES

1. Liang, G., et al.: The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Trans. Power Syst. 32(4), 3317–3318 (2017)
2. He, H., Yan, J.: Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Physical Systems: Theory & Applications. 1(1), 13–27 (2016)
3. National Institute of Standards and Technologies (NIST): Guidelines for smartgrid cybersecurity. NIST Special Publication, Gaithersburg (2014). http://www.dx.doi.org/10.6028/NIST.IR.7628r1
4. Ghosh, S., Sampalli, S.: A survey of security in SCADA networks: Current issues and future challenges. IEEE Access 7, 135812–135831 (2019). http://dx.doi.org/10.1109/access.2019.2926441
5. Tan, S., et al.: Survey of security advances in smart grid: a data driven approach. IEEE Communications Surveys & Tutorials. 19(1), 397–422 (2017). https://doi.org/10.1109/COMST.2016.2616442
6. ISO/IEC 15408.: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, 1(3.1), 15–35 (2017). https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
7. Monticelli, A.: State Estimation in Electric Power Systems: A Generalized approach, vol. 1, 1st ed. Springer (1999)

8. Deng, R., et al.: False data injection on state estimation in power systems-attacks, impacts, and defence: a survey. IEEE Trans. Industr. Inform. (2017)
9. Tan, Y., et al.: Cyber-attack on overloading multiple lines: a bilevel mixed-integer linear programing model. IEEE Trans. Smart Grid. 9(2), 1534–1536 (2018)
10. Chung, H.M., et al.: Local cyber-physical attack for masking line outage and topology attack in smart grid. IEEE Trans. Smart Grid (2018)
11. Yang, Q., Chang, L., Yu, W.: On false data injection attacks against Kalman filtering in power system dynamic state estimation. Secur. Commun. Network. 9(9), 833–849 (2016)
12. Gabbar, H.A., Dinavahi, V.: On false data injection attack against dynamic state estimation on smart power grids. In: 5th IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa (2017)
13. Karimipour, H., Dinavahi, V.: Robust massively parallel dynamic state estimation of power systems against cyber-attack. IEEE Access. 6, 2984–2995 (2017)
14. Sailik, S., et al.: 'A survey of moving target defence for networks'. IEEE Commun. Surv. Tutor. (2020)
15. ChengHong-Qi, L., et al.: Moving target defence: a survey. Hindawi Security and Communication Networks (2018)
16. Omur, O., Weerakkody, S., Bruno, S.: Moving target defence: a survey. In: IEEE International Conference on Smart Grid Communications (2018)
17. Heydari, V.: Moving target defence for securing SCADA communications. IEEE Access (2020)
18. Wang, S., Ren, W., Al.Saggaf, U.M.: Effects of switching network topologies on stealthy false data injection attacks against state estimation in power networks. IEEE Syst. J. 11(4), 2640–2651 (2015)
19. Morrow, K.L. et al.: Topology perturbation for detecting malicious data injection. In: 2012 45th Hawaii International Conference on System Sciences (2012)
20. Liu, C., et al.: Reactance perturbation for enhancing detection of FDI attacks in power system state estimation. In: 2017 IEEE Global conference on signal and information processing (GlobalSIP) (2017)
21. Li B., et al.: On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices. IEEE Trans Indust Inform. 16(2), 854–864 (2019). http://dx.doi.org/10.1109/tii.2019.2922215
22. Tian, J. et al.: Enhanced hidden moving target defence in smart grids. IEEE Trans. Smart Grid. 10(2), 2208–2223 (2019)
23. Higgins, M., Teng, F., Parisini, T.: Stealthy MTD against unsupervised learning-based blind FDI attacks in power systems. IEEE Trans. Inf. Forensics Secur. (2020). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9207760
24. Lakshminarayana, S., Yau, D.K.Y.: Cost-Benefit analysis of Moving-Target defence in power grids. In: Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018, pp. 139–150.Institute of Electrical and Electronics Engineers Inc. (2018)
25. Tamba, T.A., Hu, B., Nazaruddintld, Y.Y.: An actuator intrusion detection mechanism for event-triggered moving target Defence control (2019)
26. Lakshminarayana, S., Yau, D.K.Y.: Cost-benefit analysis of moving-target defence in power grids. IEEE Trans. Power. Syst., 1 (2020). https://ieeexplore.ieee.org/document/9144465/
27. Boneh, D., Demillo, R.A., Lipton, R.J.: On the importance of checking computations. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 37–51. Springer, Heidelberg (1997). https://www.researchgate.net/publication/2409434
28. Kocher, P.C.: Timing attacks on implementations of Diie-Hellman, RSA, DSS, and other systems. Cryptography Research Inc, San Francisco (1996). https://paulkocher.com/doc/TimingAttacks.pdf
29. Kocher, P., Jaaee, J., Jun, B.: 'Differential power analysis'. Crytograph Research Inc. San Fransico (1999). https://dl.acm.org/doi/10.5555/646764.703989
30. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. (2011)
31. Hug, G., Giampapa, J.A.: Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans. Smart Grid (2012)
32. Wood, A.J., Wollenberg, B.F., Sheblé, G.B.: Power generation, operation, and control. Wiley (2014). http://ebookcentral.proquest.com/lib/imperial/detail.action?docID=1418364
33. Multos Inc: Multos trust anchor Website. Multos, London (2020). https://www.multos.com/
34. Multos Inc: MULTOS trust anchor development board website. Multos, London (2020). https://www.multos.com/dev/_boards/devboard/_details
35. Mayes, K., Markantonakis, K.: Smart Cards, Tokens, Security and Applications, vol. 1, 1st ed. Springer, London (2017). Chapter 17'
36. Mayes, K., Babbage, S., Maximov, A.: Performance evaluation of the new TUAK mobile authentication algorithm. In: Proceedings of ICONS16: ICONS/EMBEDDED, pp. 38–44 (2016)
37. Mayes, K.: Performance of authenticated encryption for payment cards with Crypto Co-processors. In: Proceedings of ICONS17: ICONS/EMBEDDED, pp. 1–9 (2017)
38. Mayes, K.: Performance evaluation and optimisation for Kyber on the MULTOS IoT trust-Anchor. In: Proceedings of IEEE SmartIoT. Beijing, pp. 1–8 (2020)
39. EMVco, LLC: EMVco payment processing website. EMVco LCC, London (1999). https://www.emvco.com/
40. IEC: '19772 Information technology - security techniques - authenticated encryption'. International Electrotechnical Commission, London (2009)
41. Taylor, J.W., McSharry, P.E.: Short-term load forecasting methods: an evaluation based on European data. IEEE Trans. Power Syst. 22(4), 2213–2219 (2007)
42. Zimmerman, R.D., Murillo.Sánchez, C.E., Thomas, R.J.: MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans. Power. Syst. (2011)
43. National, G.: Electricity ten year statement. National Grid, London (2017). https://www.nationalgrideso.com/research-publications/electricity-ten-year-statement-etys

How to cite this article: Higgins M, Mayes K, Teng F. Enhanced cyber-physical security using attack-resistant cyber nodes and event-triggered moving target defence. *IET Cyber-Phys. Syst., Theory Appl*. 2021;6:12–26. https://doi.org/10.1049/cps2.12002