Mitigating Synchronized Hardware Trojan Attacks in Smart Grids

Chenglu Jin
University of Connecticut
Storrs, Connecticut 06269
chenglu.jin@uconnn.com

Lingyu Ren
University of Connecticut
Storrs, Connecticut 06269
lingyu.ren@uconn.edu

Xubin Liu
University of Connecticut
Storrs, Connecticut 06269
xubin.liu@uconn.edu

Peng Zhang
University of Connecticut
Storrs, Connecticut 06269
peng.zhang@uconn.edu

Marten van Dijk
University of Connecticut
Storrs, Connecticut 06269
marten.van_dijk@uconn.edu

ABSTRACT

A hardware Trojan is a malicious circuit inserted into a device by a malicious designer or manufacturer in the circuit design or fabrication phase. With the globalization of semiconductor industry, more and more chips and devices are designed, integrated and fabricated by untrusted manufacturers, who can potentially insert hardware Trojans for launching attacks after the devices are deployed. Moreover, the most damaging attack in a smart grid is a large scale electricity failure, which can cause very serious consequences that are worse than any disaster. Unfortunately, this attack can be implemented very easily by synchronized hardware Trojans acting as a collective offline time bomb; the Trojans do not need to interact with one another and can affect a large fraction of nodes in a power grid. More sophisticatedly, this attack can also be realized by online hardware Trojans which keep listening to the communication channel and wait for a trigger event to trigger their malicious payloads; here, a broadcast message triggers all the Trojans at the same time.

In this paper, we address the offline synchronized hardware Trojan attack, as it does not require the adversary to penetrate the power grid network for sending triggers. We classify two types of offline synchronized hardware Trojan attacks as type A and B: type B requires communication between different nodes, and type A does not. The hardware Trojans needed for type B turn out to be much more complex (and therefore larger in area size) than those for type A. In order to prevent type A attacks we suggest to enforce each power grid node to work in an unique time domain which has a random time offset to Universal Coordinated Time (UTC). This isolation principle can mitigate type A offline synchronized hardware Trojan attacks in a smart grid, such that even if hardware Trojans are implanted in functional units, e.g. Phasor Measurement Units (PMUs) and Remote Terminal Units (RTUs), they can only cause a minimal damage, i.e. sporadic single node failures. The proposed solution only needs a trusted Global Positioning System (GPS) module which provides the correct UTC together with small additional interface circuitry. This means that our solution can be used to protect the current power grid infrastructure against type A offline attacks without replacing any untrusted functional unit, which may already have embedded hardware Trojans.

CPSR-SG 2017, Pittsburgh, PA USA

978-1-4503-4978-9/17/04…$15.00
DOI: 10.1145/3055386.3055394

CCS CONCEPTS

•Security and privacy →Malicious design modifications;

KEYWORDS

Hardware Trojan, Supply Chain Management, Smart Grid, Synchronization

ACM Reference format:
Chenglu Jin, Lingyu Ren, Xubin Liu, Peng Zhang, and Marten van Dijk. 2017. Mitigating Synchronized Hardware Trojan Attacks in Smart Grids. In *Proceedings of The 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, Pittsburgh, PA USA, April 2017 (CPSR-SG 2017),* 7 pages.
DOI: 10.1145/3055386.3055394

1 INTRODUCTION

Recently circuit manufacturing has been outsourced to untrusted manufacturers who can implant malicious circuits of their choice in fabricated circuits during manufacturing. This means that without extensive testing for hardware Trojans on each fabricated device, nobody is able to find a hardware Trojan embedded in a fabricated device. Therefore these untested/untrusted devices used in the field undermine the security of the entire power grid. Research on hardware Trojans has been active in academia and industry for more than one decade [6, 14, 24]. One paper even discovers hardware Trojans implanted in military devices, which validates this threat to homeland security [23]. We also mention the possibility of hardware Trojans which implement 'kill switches' [2].

The smart grid, as a critical infrastructure of one country, is very vulnerable to hardware Trojan attacks, since this problem has not gained sufficient attention in power grid design. In particular, if all implanted hardware Trojans in a smart grid can get activated at the same time (due to access to synchronized time), then this collection of Trojans acts as a time bomb to destroy the functionality of a large fraction of nodes in the bulk power grid. This can lead to huge damage and a possible cascading of this power failure to other

parts of the power grid, such as the 2003 Italian blackout [18], 2003 U.S. Northeastern power outage [20], 2011 Southwest blackout [10], and 2015 Ukraine blackout [19].

We introduce the following classification of synchronized hardware Trojan attacks:

Offline synchronized hardware Trojan attacks – Type A. If all implanted hardware Trojans need to be triggered at the same time, then they need some method to properly synchronize with each other. If *no malicious communication* is allowed in the network, then, since a Global Positioning System (GPS) module is one important module in nearly every critical node of a bulk power grid and many functional modules need Universal Coordinated Time (UTC) provided by the GPS module to synchronize with each other for functional reasons, the GPS provides a perfect way for them to synchronize with UTC. For example, multiple Phasor Measurement Units (PMUs) need to sample the current and voltage signals using the same time reference to calculate the phase angles in a region for stability control. A hardware Trojan in a PMU can just take the UTC from the GPS module and trigger itself when a previously set trigger time arrives. In this way, all the PMUs can corrupt at the same time, and no one will notice any symptom before the power failure actually happens.

In order to prevent such an offline synchronized attack, we propose an additional interface circuitry which is initialized by the power companies with a unique random offset and adds this offset to the time information provided by the GPS module. As a result, each node in the power grid can be considered to work in a separate time domain, and none of them knows the current UTC and the time domain of other nodes. Obviously, this time domain isolation can prevent the hardware Trojans in different nodes being triggered at the same time. To make this system usable, all the time offsets should be stored in the control center, such that this control center can adjust the time value in the commands for each node and correct the time information in all the received messages. The system is shown in Fig.1.

Offline synchronized hardware Trojan attacks – Type B. If malicious communication between hardware Trojans is possible, then they can synchronize their actions without access to current UTC. Here, the meaning of offline is that there is no online connection from an adversarial control center to Trojans. If communication happens over the smart grid network layer, then communication modules should embed a trusted formally verified Finite State Machine (FSM) which intercepts and interprets command sequences so that the network of FSMs can discover and prevent suspicious looking communication patterns which are *synchronized in time*. If specifically designed for the smart grid, this goes beyond ordinary intrusion detection systems which either learns malicious communication patterns based on machine learning (SVM or data stream mining) applied to a smart grid data set or detects malicious patterns based on smart grid specific rules [9, 21, 34]. We leave it as an open problem to design practical FSMs that prevent type B attacks where communication is over the network layer and to design countermeasures for type B attacks where communication between Trojans is over a covert channel over the power lines [11].

We notice that type A and B offline synchronized hardware Trojan attacks require the attacker to set the (approximate) future time at which the attack should occur before the Trojans are manufactured. This means that the attacker loses control and the attack will happen at that future time no matter improvements of the relationship between the attacker and country where the power grid resides. This excludes a rational adversary from initiating such an attack – it does not exclude the psychopathic attacker. (If one does not believe in dealing with such a psychopathic manufacturer, then there is no need to protect against type A or B offline synchronized hardware Trojan attacks since according to the above argument only a psychopathic manufacturer would proceed doing this.)

Online synchronized hardware Trojan attacks. If the trigger signal is sent from an unauthorized source outside of the existing power grid network (the meaning of online), then this adversary first needs to intrude the network. In order to prevent a successful attack we need an intrusion detection system, which has been well studied for smart grids in [9, 21, 34]. It is important to note, that an online synchronized hardware Trojan attack of this flavor should be compared to the difficulty of a remote attacker who has already penetrated the network to exploit vulnerabilities or insert a software Trojan (i.e. malware) in the software stack rather than having hardware Trojans in place.

The rest of this paper analyses mitigation of type A and discusses mitigation of type B *offline* synchronized hardware Trojan attacks. We do not further discuss the online synchronized hardware Trojan attack and leave this as an open problem for future work.

1.1 Contributions

In this paper, we make the following main contributions:

(1) We raise the alarm of coordinated hardware Trojan attacks in a power grid, whose study is long overdue. It is important to question the trustworthiness of the underlying hardware when we are studying the security of the software running on top of it.

(2) We propose to isolate the time domain of each node to prevent type A offline hardware Trojans from being activated at the same time. This converts a failure of the entire power grid to sporadic single node failures (sporadic since the random offsets may differ in years).

(3) Effectively, our solution reduces the trusted computing base with respect to a coordinated type A offline hardware Trojan attack from the need for trust in all the devices in nodes of a power grid to trust in the GPS module (with a small additional interface circuitry) in each node. This significantly enhances the security of the entire power grid and reduces the testing time before deployment.

(4) Our solution is applicable to the current power grid infrastructure to prevent a synchronized type A offline hardware Trojan attack from happening. There is no need to replace any functional unit in the power grid, even if units are suspicious and may be malicious. It just requires an additional small interface circuit and a software update in the control center.

1.2 Organization

Sec.2 introduces the current state-of-the-art of hardware Trojans research and the synchronization issues in a smart grid. Our solution for preventing type A offline attacks is presented and analyzed in

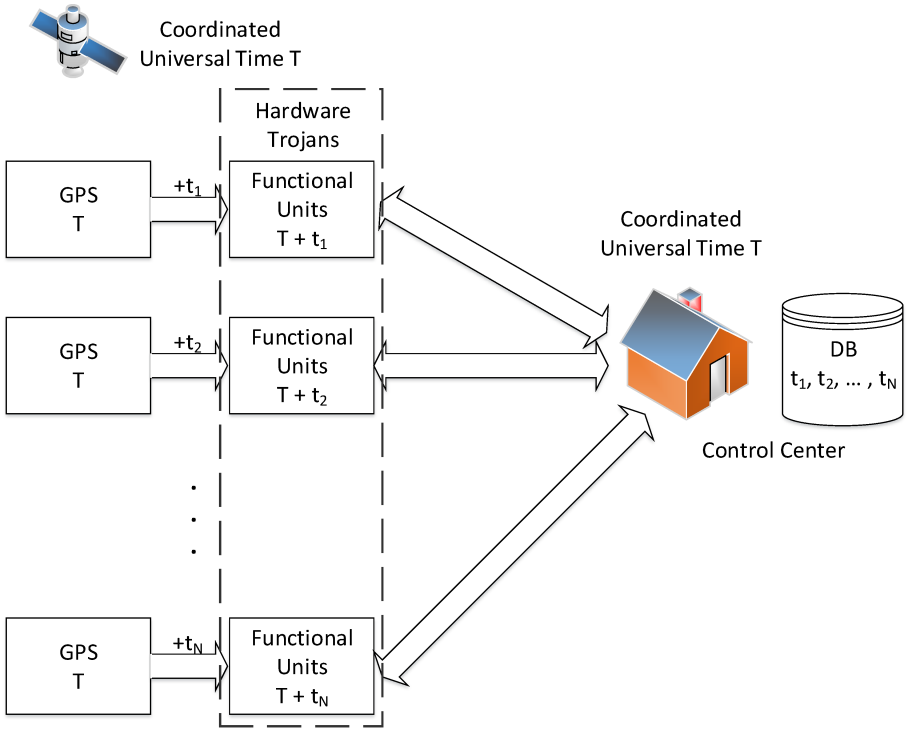

Figure 1: While the GPS modules are providing the correct UTC T, each functional unit i is working in its own isolated time domain $T + t_i$. The control center stores all the time offsets in its database. The dotted block indicates where the hardware Trojans can possibly be inserted into.

Sec.3. Sec.4 explains strategies towards mitigation of type B attacks in more detail. Finally, Sec.5 concludes the paper and discusses the reality of type A or B attacks.

2 BACKGROUND AND RELATED WORK

2.1 Hardware Trojans: Attacks and Defenses

Hardware Trojan research has been active in the hardware security research community for more than a decade. Due to the creativity of attackers, new hardware Trojan designs continuously emerge that escape detection from state-of-the-art detection schemes and methods [4, 15, 28, 30]. Therefore, it is very difficult to guarantee one device is completely free of hardware Trojans.

Another drawback of the current state-of-the-art detection schemes is the trade-off between detection probability and computational complexity. For Trojans inserted in the design phase, the complexities of state-of-the-art detection tools (e.g. HaTCh [14], FANCI [26] and VeriTrust [29]) grow very fast if they want to detect the hardware Trojans proposed in [15, 30] with high probability. Also, for Trojans inserted in the fabrication phase, post-silicon detection schemes usually require extensive investigation to compare some specific characteristics (e.g. power consumption [3] and path delay [17]) of each chip with a golden/trusted copy. Typically, these post-silicon detection schemes can only perform testing on some random samples on one wafer, because it is too time-consuming to test all the samples.

Summarizing, it is very challenging to completely eliminate the threats of hardware Trojans in power system hardware devices.

Supply Chain Management: This paper fits a larger discussion on secure supply chain management [12] of ICs in power grid devices during design, fabrication, assembly, distribution, lifetime, recycling and end-of-life. Since insertion of hardware Trojans in the supply chain is difficult and costly (if not impossible) to detect (during testing), this paper proposes countermeasures and suggestions for future work to eliminate this threat.

2.2 Synchronization in Smart Grids

Nowadays, the North America power grid is increasingly relying on synchronized clocks, especially the atomic clocks on GPS satellites, to enable real-time accurate monitoring and control for maintaining stability and reliability of our continent-wide interconnected bulk power grid. This is justifiable because several major blackouts, such as the two 1996 western electric grid blackouts and the 2003 eastern electric grid blackout [20], could have been prevented or alleviated if there existed wide-area synchronized situational awareness and control of disturbance events in the bulk power grid. In late 1990s, PMU was invented and, for the first time, achieved synchronized measurement in power grid by time-stamping each measurement (e.g., voltage, current, and frequency) according to a common time

reference in UTC provided by GPS [5, 8, 22]. PMUs allow measurements from different regions and utilities to be synchronized and, if networked, could provide unprecedented observability and controllability of the entire North American interconnection [1, 27, 31–33]. For this reason, thousands of PMUs haven been installed in U.S. power utilities grids with the support from Department of Energy and more devices are to be deployed in the coming years.

Another trend is to introduce GPS signals to other measurement and control devices in the power grids such as remote terminal units (RTUs). RTUs are still the most-widely used automation devices in substations even though their accuracy and data transmitting rates are much lower than those of PMUs. Equipped with GPS receivers, RTUs will be able to provide much more accurate and useful information for the supervisory control and data acquisition (SCADA) systems [13, 22]. Therefore, it is foreseeable that synchronized phasor signals will soon be widely used across power generation (e.g., large hydro and thermal power plants, distributed generation systems such as PV power systems and wind farms), transmission (especially substation automation systems), and distribution grids (e.g., smart meters and sensors).

In summary, synchronized signals are made available to an increasing number of power system hardware devices such as RTUs, PMUs and other GPS-enabled devices. The widely available synchronization signals, however, enables hardware Trojans implanted in power system hardware devices to perform coordinated attacks that can cause major blackouts and catastrophic cascading failures in North American power grids.

3 TYPE A: MITIGATION STRATEGY

We analyze type A offline synchronized hardware Trojan attacks where the Trojans do not attempt to communicate which each other.

3.1 Proposed Solution

In each node of a power grid, the coordinated universal time T is provided by the GPS module, and it is used in functional units, such as PMUs and RTUs. If a malicious manufacturer embeds hardware Trojans in the PMUs, then each Trojan just needs to trigger its payload at the same time $T_{trigger}$ to cause a huge synchronized and coordinated blackout in the corresponding power grid.

Given the challenges we are facing in hardware Trojan detection as described in Sec.2, we suggest to defeat synchronized hardware Trojan attacks by preventing access to the UTC in the first place so that each hardware Trojan is at a loss when time $T_{trigger}$ occurs. We propose to isolate each hardware Trojan by isolating the node with the functional units in its own time domain (reference framework) as shown in Figure 1. We propose to add a time offset t to the time provided by the GPS receiver. As a result, instead of getting correct coordinated universal time T from the GPS receiver, the corresponding functional unit receives time $T + t$.

Let $\{t_1, t_2, \cdots, t_N\}$ be the time offset of nodes 1 to N in the power grid. These time offsets are initialized as random numbers by the control center and are stored in a database. Therefore, in each node, no functional unit knows the correct time, except the GPS receiver. In this way, the functional units in different power grid nodes are working with different time domains, and as a result they cannot synchronize with each other. Even when a specific trigger time is achieved in one node, only that node will fail. This is just a single node failure which a power grid can tolerate and quickly recover from. The time offsets t_i can be randomly chosen from a large multi-year range so that node failures will be spread out over a long time window. Therefore, a huge blackout is converted into sporadic single node failures which mitigate damage to an acceptable minimum.

Case Study: If we are considering a time signal encoded in IRIG-B standard [25], which is a widely used time code standard, the overall time offset space is 100 years. As a result, if the time offset is uniformly distributed, then single node failures will also be uniformly distributed over 100 years.

3.2 Usability

As discussed in Sec.2, in the smart grid we do need some functional units to be synchronized over the entire power grid. For example, PMUs do need to sample the power signal using the same time reference for phase measurement. However, in our proposed system, PMUs do not have access to the correct UTC T. In order to fix this issue, the control center should adjust all the commands sent to the PMUs to the time domain of each destination PMU. Since the control center knows all the offsets $\{t_1, t_2, \cdots, t_N\}$, it can adjust the commands sent to the PMUs and also correct the messages received from PMUs. For example, after receiving data from node i, the control center can shift the time tag by t_i so that the data will fit into i's UTC frame. In this way, we can still guarantee that all measurements from different PMUs still have correct UTC tags but none of the PMUs knows the exact UTC since they are obfuscated by their offsets similar to a one-time-pad encryption.

Notice that our proposed solution only incurs very minimal changes to the current power grid design. We can still use off-the-shelf GPS modules and other functional units in our system and just add one small interface at the time output of GPS modules. All the time offsets can be programmed when the devices are deployed, and the control center just needs to adjust their commands according to the offset of each node. This also requires a very minimal change in the control program. Moreover, our solution can be directly applied to the current power grid infrastructure without replacing any untrusted functional unit. This dramatically reduces the cost for upgrading the current system to prevent a synchronized hardware Trojan attack.

3.3 Security Analysis

In the above discussion, (besides the type A offline assumption assuming no inter Trojan communication) we made a very important assumption that the GPS module is trusted. This implies that the GPS module is free of hardware Trojans itself and is always providing the correct UTC to the other functional units. Essentially, we reduce the trusted computing base from trusting every single node in the entire power grid to the following three trust assumptions:

- All the GPS modules in the power grid should be trusted and provide correct UTC.
- The additional interface circuitry is trusted.
- The software running on functional units is trusted.

How can we guarantee the trustworthiness of a GPS module and additional interface circuitry? We suggest two possible approaches:

(1) One can perform extensive testing on the GPS module and the additional interface, see [3, 14, 17, 26]. This may be acceptable since only the GPS modules and additional interfaces form the hardware trusted computing base for guaranteeing reliable operation of the power grid in an adversarial environment. It significantly reduces the testing time before deployment because we only need to test GPS modules and additional interfaces, instead of testing every single module in the power grid. Hence, it may be worth the effort to test GPS modules and the simple interface circuitry thoroughly.

(2) Since we need to assemble GPS modules and other functional units in a trusted environment and add an extra interface between them, we can ask one trusted manufactuer to fabricate all the GPS modules together with its interface and let the untrusted manufacturers fabricate other functional units. This exploits the idea of split manufacturing [16]. The concept of split manufacturing is that instead of manufacturing one entire chip by one untrusted manufacturer, one splits the chip design into two layers and asks two untrusted manufactures to fabricate one of the layers individually. After fabrication, one can assemble these two layers in a trusted environment. The main assumption behind split manufacturing is that these two untrusted manufacturers are not going to collude with each other and the cost of assembly is much lower than that of (outsourced) manufacturing.

The third assumption ought to be naturally satisfied as it is needed to guarantee that there is no malicious software which has access to the current UTC, otherwise a standalone software Trojan (called malware) can cause the failure of the entire power grid as well. We make the third assumption explicit since this implies that hardware Trojans cannot access UTC (or any other trigger signal/event) by observing or connecting to executing software (trusted software would not harvest UTC from connecting to the internet as it can already access the GPS unit).

Implicitly, we also assume that hardware Trojans inside functional units do not contain a real time clock (e.g. a hardware Trojan does not have a GPS module in it), because this would be too large in size and can therefore easily be detected (by coarse grained hardware inspection).

With all the above security assumptions, hardware Trojans become isolated from access to UTC implying we are able to guarantee that **offline hardware Trojans without the capability to communicate together will not cause power failure of the entire power grid**.

Notice that we do not require the time offsets to be secret, because the hardware Trojans are produced before the random time offsets are generated. We do require the time offsets to be random so that an adversary cannot predict these offsets in advance and, hence, initialize hardware Trojans accordingly.

4 TYPE B: TOWARDS MITIGATION

We now analyze type B offline synchronized hardware Trojan attacks where the Trojans are communicating with each other. This allows the Trojans to agree together on a shared time reference so that they can synchronize their attack.

The countermeasure presented in the previous section isolates hardware Trojans from one another, yet, they can start their individual clock counters as soon as they are power-up and employed in the field. Each Trojan triggers its payloads once its individual counter reaches a preset max counter value. The hardware Trojans will be employed at different moments over time, however, note that these moments will not be uniformly distributed over a period of 100 years as in our case study, instead they are distributed over a much shorter timespan leading to a higher rate of single node failures.

If Trojans can communicate with each other, then they can coordinate their individual clocks and collectively trigger their payloads in a synchronized way. Self-synchronization requires a master-slave protocol: Each hardware Trojan can be both master and slave. They all start counting after powering up at initialization (as explained above). Each Trojan starts out as a slave. The first Trojan reaching a preset max counter value changes its state to master and starts communicating with all other Trojans (making use of other Trojans for forwarding messages). This allows all Trojans to agree on a common time reference and within this reference frame they collectively trigger their malicious payloads at the same coordinated time (as indicated by the master Trojan).

In order to mitigate this type of attack, malicious communication among Trojans should be prevented. In particular, Trojans can have access to or are embedded in communication interface modules (which define the smart grid network layer). In order to prevent malicious communication between *communication modules*, such modules *should have a trusted formally verified Finite State Machine (FSM) which interprets commands and flags suspicious communication patterns*. As a concrete example, a reset command should be verified to come from the centralized smart grid control center. We notice that these FSMs will need to communicate with one another so that they can detect command patterns which occur at the same time across many nodes in the smart grid – and this should be flagged as unlikely and prevented. In order to increase the difficulty for a master Trojan to trigger other Trojans, we suggest to use devices from noncollaborating manufacturers such that neighboring nodes in the network topology originate from the different manufacturers. Assuming nodes do not simply forward messages to other nodes (the FSMs suggested here should prevent this), master trigger signals will be blocked since devices fabricated by different noncollaborating manufactures cannot interpret one another's trigger signals. These countermeasures are not as simple as the countermeasure proposed for preventing type A offline attacks – we leave it as an open problem to develop practical FSMs in communication modules that prevent type B attacks where malicious communication is over the smart grid network layer.

The previous section discusses how to isolate Trojans from current UTC time, which is received by the GPS module. Other communication to Trojans can be over the smart grid network layer itself as discussed above or if possible, by means of a hidden covert channel over the power lines. The latter assumes hardware Trojans are able to communicate over the power lines itself: such communication is possible [11] and possibly easy to implement if used for forwarding a specific trigger signal. We also leave the analysis of this type of communication among hardware Trojans as an open problem.

As a final remark we notice that hardware Trojans for type B attacks are necessarily much more complex than the simple hardware Trojans for type A attacks. Hardware Trojans for type B attacks are likely also much more complex than those needed in an online synchronized hardware Trojan attack as the manufacturer could add a backdoor which allows read/write of memory at a later moment when the smart grid network has been successfully penetrated. This means that type B Trojans will be larger in size as compared to type A Trojans and they can therefore more easily be detected by hardware inspection.

5 CONCLUSION

This paper highlights the security threat from synchronized hardware Trojans which can cause a power failure of the entire power grid. We classified three types of synchronized attacks: 'type A offline' where Trojans do not communicate with each other, 'type B offline' where Trojans do communicate with each other but without online communication with an unauthorized source outside of the existing power grid network, and 'online' where Trojans can receive a trigger signal from an unauthorized outside source.

For preventing (type A) offline synchronized hardware Trojan attacks where Trojans do not communicate with each other, this paper proposes to add a random time offset to the time provided by a GPS module. This prevents offline hardware Trojans in functional units across power grid nodes from being activated at the same time. The trustworthiness of the entire system is bootstrapped from the trustworthiness of GPS modules together with their simple extra interfaces, but no other hardware needs to be trusted. This makes the proposed solution practical and economically feasible to implement and allows a cheap upgrade of current smart grid infrastructure to prevent synchronized hardware Trojan attacks. Also, it implies a reduction in testing time before deployment for new nodes in the future (since only the GPS modules with their extra interfaces need to be tested).

ACKNOWLEDGMENTS

Lingyu Ren and Peng Zhang are supported by the National Science Foundation under Grant No. 1611095.

REFERENCES

[1] Ali Abdollahi, Peng Zhang, Hui Xue, and Sherwin Li. 2013. Enhanced subspace-least mean square for fast and accurate power system measurement. *IEEE Transactions on Power Delivery* 28, 1 (2013), 383–393.
[2] Sally Adee. 2008. The hunt for the kill switch. *iEEE SpEctrum* 45, 5 (2008), 34–39.
[3] Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. 2007. Trojan detection using IC fingerprinting. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE, 296–310.
[4] Georg T Becker, Francesco Regazzoni, Christof Paar, and Wayne P Burleson. 2013. Stealthy dopant-level hardware trojans. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 197–214.
[5] Ken Behrendt, Ken Fodero, and others. 2006. The perfect time: An examination of time-synchronization techniques. In *Proc. 33rd Ann. West. Prot. Rel. Conf., Spokane, WA, USA*. Citeseer, 17–19.
[6] Swarup Bhunia, Michael S Hsiao, Mainak Banga, and Seetharam Narasimhan. 2014. Hardware Trojan attacks: threat analysis and countermeasures. *Proc. IEEE* 102, 8 (2014), 1229–1247.
[8] MM Eissa, M Elshahat Masoud, and M Magdy Mohamed Elanwar. 2010. A novel back up wide area protection technique for power transmission grids using phasor measurement unit. *IEEE Transactions on Power Delivery* 25, 1 (2010), 270–278.
[9] Mustafa Amir Faisal, Zeyar Aung, John R Williams, and Abel Sanchez. 2015. Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study. *IEEE Systems Journal* 9, 1 (2015), 31–44.
[10] NERC Ferc. 2012. Arizona-southern california outages on 8 September 2011: causes and recommendations. *FERC and NERC* (2012).
[11] Stefano Galli, Anna Scaglione, and Zhifang Wang. 2011. For the grid and through the grid: The role of power line communications in the smart grid. *Proc. IEEE* 99, 6 (2011), 998–1027.
[12] Ujjwal Guin, Daniel DiMase, and Mohammad Tehranipoor. 2014. Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. *Journal of Electronic Testing* 30, 1 (2014), 9–23.
[13] Suphan Gulpanich, Arjin Numsomran, Vittaya Tipsuwanporn, and Kitti Tirasesth. 2005. Distributed control of network devices with remote terminal units. In *Industrial Technology, 2005. ICIT 2005. IEEE International Conference on*. IEEE, 823–828.
[14] Syed Kamran Haider, Chenglu Jin, Masab Ahmad, Devu Manikantan Shila, Omer Khan, and Marten van Dijk. 2017. Advancing the State-of-the-Art in Hardware Trojans Detection. *IEEE Transactions on Dependable and Secure Computing* (2017).
[15] Syed Kamran Haider, Chenglu Jin, and Marten van Dijk. 2016. Advancing the state-of-the-art in hardware trojans design. *arXiv preprint arXiv:1605.08413* (2016).
[16] Richard Wayne Jarvis and Michael G McIntyre. 2007. Split manufacturing method for advanced semiconductor circuits. (March 27 2007). US Patent 7,195,931.
[17] Yier Jin and Yiorgos Makris. 2008. Hardware Trojan detection using path delay fingerprint. In *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*. IEEE, 51–57.
[18] Chris W Johnson. 2007. Analysing the causes of the Italian and Swiss blackout, 28 th september 2003. In *Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems-Volume 86*. Australian Computer Society, Inc., 21–30.
[19] Robert M Lee, Michael J Assante, and Tim Conway. 2016. Analysis of the cyber attack on the Ukrainian power grid. *SANS Industrial Control Systems* (2016).
[20] B Liscouski and W Elliot. 2004. Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations. *A report to US Department of Energy* 40, 4 (2004).
[21] Robert Mitchell and Ray Chen. 2013. Behavior-rule based intrusion detection systems for safety critical smart grid applications. *IEEE Transactions on Smart Grid* 4, 3 (2013), 1254–1263.
[22] M Jaya Bharata Reddy, D Venkata Rajesh, Pathirikkat Gopakumar, and Dusmanta Kumar Mohanta. 2014. Smart fault location for smart grid operation using RTUs and computational intelligence techniques. *IEEE Systems Journal* 8, 4 (2014), 1260–1271.
[23] Sergei Skorobogatov and Christopher Woods. 2012. Breakthrough silicon scanning discovers backdoor in military chip. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 23–40.
[24] Mohammad Tehranipoor and Farinaz Koushanfar. 2010. A survey of hardware trojan taxonomy and detection. *IEEE Design & Test of Computers* 27, 1 (2010).
[25] TELECOMMUNICATIONS and TIMING GROUP. 2016. Overview of IRIG-B Time Code Standard, Technical Report. http://www.cyber-sciences.com/documents/TN-102_IRIG-B.pdf. (2016).
[26] Adam Waksman, Matthew Suozzo, and Simha Sethumadhavan. 2013. FANCI: identification of stealthy malicious logic using boolean functional analysis. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 697–708.
[27] Hui Xue and Peng Zhang. 2012. Subspace-least mean square method for accurate harmonic and interharmonic measurement in power systems. *IEEE Transactions on Power Delivery* 27, 3 (2012), 1260–1267.
[28] Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, and Dennis Sylvester. 2016. A2: Analog malicious hardware. In *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 18–37.
[29] Jie Zhang, Feng Yuan, Linxiao Wei, Yannan Liu, and Qiang Xu. 2015. VeriTrust: Verification for hardware trust. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 34, 7 (2015), 1148–1161.
[30] Jie Zhang, Feng Yuan, and Qiang Xu. 2014. Detrust: Defeating hardware trust verification with stealthy implicitly-triggered hardware trojans. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 153–166.
[31] Peng Zhang, Hui Xue, and Rengang Yang. 2011. Shifting window average method for accurate frequency measurement in power systems. *IEEE Transactions on Power Delivery* 26, 4 (2011), 2887–2889.
[32] Peng Zhang, Hui Xue, Rengang Yang, and Jian Zhang. 2014. Shifting window average method for phasor measurement at offnominal frequencies. *IEEE Transactions on Power Delivery* 29, 3 (2014), 1063–1073.
[33] Peng Zhang, Ning Zhou, and Ali Abdollahi. 2013. A generalized subspace least mean square method for high-resolution accurate estimation of power system oscillation modes. *Electric Power Components and Systems* 41, 12 (2013), 1205–1212.
[34] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C Green II, and Mansoor Alam. 2011. Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid* 2, 4 (2011), 796–808.