CIS-TC Newsletter

Communications and Information Security Technical Committee

http://cis.committees.comsoc.org/

Issue 7 – December 2020

cistc@comsoc.org

http://cis.committees.comsoc.org/newsletters

Contents

Message from the Chair

Dear CISTC Members,

I would like to sincerely welcome you to the present issue of CIS-TC Newsletter. In 2016 we started to plan it as a mean to share relevant information among the Members of our Committee twice per year to coincide with the meeting at ICC and Globecom conferences. However, the global pandemic compelled the remote rescheduling of all the IEEE 2020 events, and, consequently, our meetings has become *virtual* events; as a consequence, our Newsletter could be considered an essential way to reshape relationships within our communities via a wider and more structured social internetworking.

In this perspective, we are expected to improve to improve the level of interactive discussion by using this Newsletter as an *open* and *inclusive* platform *in progress* where all the Members of our Community are welcome to cooperative contribute to imagine *our* future. Please feel free to send us any scientifical, technical contributions or even news that you believe could be beneficial to our community. And, since Christmas is approaching and a New Year is coming, I do hope you will enjoy in reading this Issue, while spending your deserved holidays with your family and friends.

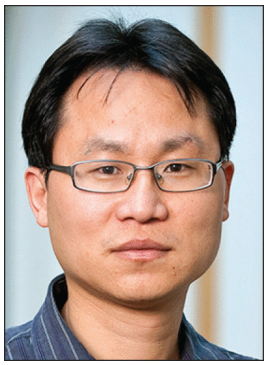
Let me conclude this message wishing you and your loved ones, on behalf of all the CIS-TC Officers, peaceful and healthy season holidays together with a renewed and prosperous 2021,

Sincerely,
Francesco Chiti
Chair of CIS-TC

CISTC Outstanding Service Award 2020

The Award Committee chaired by Professor Abderrahim Benslimane, with unanimous consent decided to give CIS-TC Outstanding Service Award 2020 to Professor Xiaodong Lin at the University of Guelph (Canada) for "his excellent contribution to security field, to ComSoc and to CISTC, where he has been Secretary, Vice-Chair and Chair".

The Committee congratulate with the Awarded and, due to the global pandemic, he will be awarded during the CIS-TC meeting held at IEEE ICC 2021 in Montreal, Canada.



Xiaodong Lin *[GS'06, M'08, SM'12, F'17] (xlin08@uoguelph.ca) received his Ph.D. degree (with the Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Canada, in 2008. He is currently an associate professor of computer science with the School of Computer Science at the University of Guelph, Canada. His research interests include communication security, computer and network security, digital forensics, privacy, software security, applied cryptography.*

Forthcoming Meeting

The next IEEE ComSoc Communication & Information Security TC (CIS-TC) meeting will be held at IEEE ICC 2021, 14-18 June 2021 (Montreal, Canada): you are more than welcome to join it and to provide your valuable contribution.

IEEE ICC
IEEE International Conference on Communications
14-18 June 2021 // Montreal, Canada
Connectivity – Security – Privacy

Featured Topics

"D-FACTS Based Proactive False Data Detection for Smart Grids: Feasibility and Limitations"

Beibei Li[1], and Rongxing Lu[2]
[1]College of Cybersecurity, Sichuan University, P.R. China
[2]Faculty of Computer Science, University of New Brunswick, Canada

Emerging as the next generation digital information network and modernized power generation, transmission, and distribution systems, smart grids are expected to enable more efficient, reliable, and sustainable power systems that can meet the demands of the 21st century and beyond. However, recent years have witnessed a sharp increase of cyber-attacks on energy industry which are becoming increasingly challenging and threatening.

Over the years, the high-profile false data injection (FDI; also known as data integrity or data deception attacks in the literature) attacks on smart grids have drawn extensive research attentions from both energy and security communities [1] - [4]. FDI attackers inject falsified data into the real-time measurements to mislead power system state estimation with an expectation to gain illicit financial gains (e.g. electricity theft) or commit sabotage acts (e.g. power outages). The success of an FDI attack is based upon attackers' knowledge of power grid connections and configurations. Unfortunately for the defenders, FDI attackers' knowledge harvesting towards power girds has been remarkably facilitated by the rapid integration of information and communications technologies and the global proliferation of powerful hacking tools. As is strictly proved that, if armed with valuable information of power grids, the knowledgeable FDI attackers are capable of constructing attack vectors that can easily circumvent the conventional state estimation based false data detection (FDD) defenses. This may make many of existing FDD defenses no longer feasible.

We have been working on defending against FDI attacks in smart grids for several years. A comprehensive survey was presented, which overviewed the problem of constructing FDI attacks, showed their associated impacts on electricity market operations, and presented countermeasures against FDI attacks [2]. We introduced a distributed host-based collaborative detection method for detecting FDI attacks in smart grids, where a conjunctive rule based majority voting algorithm was designed to collaboratively detect false measurement data inserted by compromised phasor measurement units (PMUs), and an innovative reputation system with an adaptive reputation updating algorithm was then designed to evaluate the overall running status of PMUs, by which FDI attacks can be distinctly observed [3]. We proposed a hybrid Paillier cryptosystem based approach to prevent and mitigate FDI attacks in smart grids. It is strictly proved that the critical information - power grid connections and configurations as well as the original measurement data - used for constructing FDI attacks can be well protected by using the proposed approach [4].

In our recent research efforts, we focused on the feasibility and limitations of detecting FDI attacks by using distributed flexible AC transmission system (D-FACTS) devices. We were inspired by a few recent studies, which opened the possibilities of achieving proactive FDI detection – we termed as PFDD - in smart grids by using D-FACTS devices (see Fig. 1 for the PFDD schema in smart grids). The feasibility of PFDD was probably due to the unique capability of D-FACTS devices in generating reactance perturbation, which can produce moving targets against FDI attackers. Another significant reason may lie in the

decreasing installation costs and weights of D-FACTS devices, which made it possible to widely deploy D-FACTS devices in smart grids.

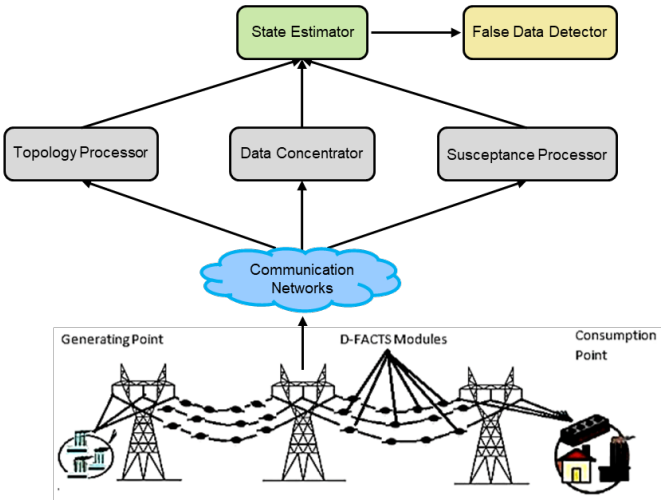
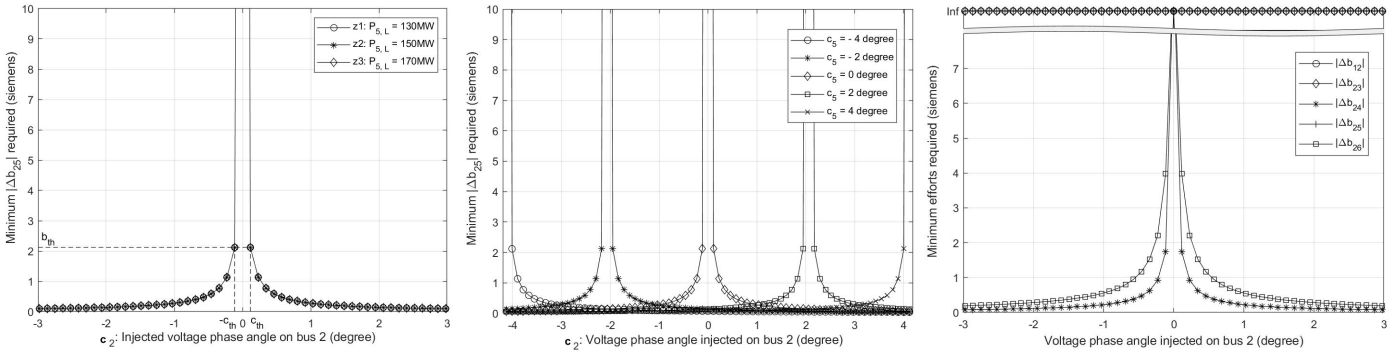


Fig. 1 The proactive false data detection (PFDD) schema with D-FACTS devices in smart grids.

However, despite of these recent developments, some significant issues regarding PFDD remain largely open, such as the number and locations of D-FACTS devices needed to facilitate the detection of FDI attacks, as well as the diverse strategies required to detect different types of FDI attacks. To solve these issues, we systematically explore the feasibility and limitations of using PFDD to detect FDI attacks in smart grids, respectively under three different types of FDI attacks, i.e., single-bus, uncoordinated multiple-bus, and coordinated multiple-bus FDI attacks.

We presented the framework for the PFDD approach, followed by an optimization problem to figure out the minimum efforts (by activating D-FACTS devices) required for detecting FDI attacks. Fig. 2 depicts the relationship between the minimum efforts versus the injected false data (i.e., degree of voltage phase angle), respectively for various types of FDI attacks. It can be observed that the PFDD approach is able to detect the existence of FDI attacks targeted on either end bus(es) (with degrees both larger than 1) of this branch, if and only if the injected phase angle difference between the two end buses is larger than a tolerance threshold. We then strictly proved that the PFDD approach is feasible to detect FDI attacks targeted on buses or super-buses with degrees larger than 1, if and only if the unknown branches cover at least a spanning tree of the power grid graph. In addition, we also carefully investigated the limitations of employing PFDD approach in detecting FDI attacks in smart grids. Findings show that, given a power grid hosting buses or super-buses with degrees equalling 1, the PFDD approach is not able to detect FDI attacks targeted on these buses or super-buses. Although being a significant theoretical limitation for the PFDD approach, it is practically not applicable for most of the smart grids, because there are usually no buses or super-buses with degrees equalling 1.

In summary, the PFDD approach is a promising approach in detecting FDI attacks in smart grids. It can be imagined that activating D-FACTS devices tuning at random intervals may catch FDI attackers by surprise. Many open issues, such as the removal of buses or super-buses with degrees equalling 1 in smart grids, or the potential effects of proactively tuning D-FACTS devices on power system stability, however, still request careful studies before such proactive detection methods could, if ever, be put into real-life applications. Investigating on such open issues shall be of our future research interest.



(a). Single-bus FDI (b). Uncoordinated multiple-bus FDI (c). Coordinated multiple-bus FDI

Fig. 2 The relationship between the minimum efforts *v.s.* the injected false data (i.e., degree of voltage phase angle).

References

[1] B. Li, G. Xiao, R. Lu, R. Deng, H. Bao, "On Feasibility and Limitations of Detecting False Data Injection Attacks on Smart Grids Using D-FACTS Devices". IEEE Transactions on Industrial Informatics, Vol. 16, No. 2, pp.854-864, 2020.

[2] R. Deng, G. Xiao, R. Lu, H. Liang, and A. Vasilakos, "False Data Injection on State Estimation in Power Systems --- Attacks, Impacts, and Defense: A Survey", IEEE Transactions on Industrial Informatics, Vol. 13, No. 2, pp. 411-423, 2017.

[3] B. Li, R. Lu, W. Wang, and R. Choo, "Distributed Host-based Collaborative Detection for False Data Injection Attacks in Smart Grid Cyber-Physical System", Journal of Parallel and Distributed Computing, Vol. 103, pp. 32-41, 2017.

[4] B. Li, R. Lu, G. Xiao, Z. Su, A. Ghorbani, PAMA: A Proactive Approach to Mitigate False Data Injection Attacks in Smart Grids, Proc. IEEE Globecom'18, Abu Dhabi, UAE, Dec. 9-13, 2018.

CIS-TC Organized Symposia

- *Communications and Information System Security Symposium* – **Globecom2020,** 7-11 December 2020, - Virtual Conference - Taipei, Taiwan (https://globecom2020.ieee-globecom.org)
- *Communications and Information System Security Symposium* – **ICC2021**, 14-18 June 2021 Montreal, Canada (https://icc2021.ieee-icc.org)

CIS-TC Affiliate Conferences

- **Conference: WiMob 2020**
  - 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2020)
  - October 12-14, 2020, Thessaloniki, Greece
  - http://www.wimob.org/wimob2020

- **Conference: CSNET 2020**
  - 4th Cyber Security in Networking Conference
  - October 21 – 23, 2020, Lausanne, Switzerland
  - https://csnet-conference.org/2020