A Fog-based Collaborative Intrusion Detection Framework for Smart Grid

Wenjuan Li[1,2], Man Ho Au[2], and Yu Wang[1⋆]

[1] Department of Computer Science, Guangzhou University, China
[2] Department of Computing, The Hong Kong Polytechnic University, China

Abstract. With the rapid development of information and communication technologies (ICT), the conventional electrical grid is evolving towards an intelligent smart grid. Due to the complexity, how to protect the security of smart grid environments still remains a practical challenge. Currently, collaborative intrusion detection systems (CIDSs) are one important solution to help identify various security threats, through allowing various IDS nodes to exchange data and information. However, with the increasing adoption of ICT in smart grid, cloud computing is often deployed in order to reduce the storage burden locally. However, due to the distance between grid and cloud, it is critical for smart grid to ensure the timely response to any accidents. In this work, we review existing collaborative detection mechanisms and introduce a fog-based CIDS framework to enhance the detection efficiency. The results show that our approach can improved the detection efficiency by around 21% to 45% based on the concrete attacking scenarios.

Keywords: Intrusion Detection, Smart Grid, Collaborative Environment, Fog Computing, Security and Trust, Time Efficiency.

1 Introduction

Conventional electrical grid is mainly used to transport electrical energy from a central power plant to many end-users by adjusting the voltage level. With the rapid growth in grid size, scale and complexity, there is an increasing need for a Smart Grid (SG), which constitutes a technological evolution through involving information and communication technologies (ICT), with the purpose of offering better capabilities in terms of reliability, efficiency and security [5], i.e., 1) it can enhance the robustness of power transmission; 2) improve the efficiency of power distribution; 3) save budgets for electric utilities; 4) and reduce Greenhouse Gas (GHG) and other gas emissions.

With the increased intelligence achieved by adopting ICT, Smart Grid also expects to improve the system's response capability under emergency. As such, it is often composed of an electric network, a digital control appliance, and an intelligent monitoring system. However, due to the distributed computing components in grids interoperation, SG may face many cyber security threats. For

⋆ Corresponding author, Email: yuwang@gzhu.edu.cn

example, the US gas pipeline was reported to be targeted by cyber attackers, where the electronic data interchange (EDI) services were affected [6]. For a concrete example, in Georgia USA, the Edwin I nuclear power plant was forced to make an emergency shutdown as long as 48 hours for the sake of a software update. This update patched the computer system but caused a lack of monitoring information, resulting in an automatic shutdown [7]. Currently, the security breaches target primarily on the aspects of confidentiality, integrity and availability in SG.

To protect a smart grid environment, intrusion detection systems (IDSs) are one basic and important security tool. Based on the detection methods, an IDS can be categorized into either rule-based detection or anomaly-based detection [36]. The former detects a potential attack by comparing the current events with its stored rules (or signatures), which contain a set of features of a (known) particular attack. The latter identifies a malicious event according to the pre-defined normal profile. While the conventional detector has no information about its protected environment in practice, it cannot identify complex and advanced threats [26]. For this sake, distributed / collaborative intrusion detection systems (DIDSs / CIDSs) are developed attempting to improve the detection performance via information exchange, i.e., obtaining more accurate result via alert aggregation.

Based on this idea, many IDS schemes are developed in the literature, by using key management, encryption, authentication, security protocol, and so on [35]. For instance, Patel et al. [33] introduced a collaborative intrusion detection and prevention system to safeguard SG with a fully distributed management structure. Liu et al. [13] designed a CIDS to identify false data injection attacks on the advanced metering infrastructure (AMI). These proposed mechanisms have shown promising performance; however, with the increasing size and scale of SG, real-time detection has become more difficult, i.e., some delay might be caused by exchanging information with controllers or cloud servers. Focused on this issue, in this work, we revise a CIDS framework using fog devices that can help improve the time efficiency of detection. In the literature, there exist few studies discussing the use of fog computing in SG. The contributions can be summarized as below.

- We propose a fog-based CIDS framework to help reduce the latency caused by the distance between SG and cloud. The fog devices can provide the capability of making decisions nearby the IDS node.
- In the evaluation, we simulate a smart grid environment and investigate our framework under both internal and external attacks. The results show that our framework can greatly improve the time efficiency of detection.

Organization. Section 2 reviews related research studies on the application of intrusion detection in smart grid. Section 3 introduces the background of smart grid and DIDS / CIDS. Section 4 details our proposed fog-based CIDS framework that uses fog devices to help enhance the efficiency of detection in SG. Section 5 shows an evaluation to explore the performance of our approach

and to validate its effectiveness under both internal and external attacks. Some open challenges are discussed in Section 6. We conclude the work in Section 7.

2 Related Work

The public research of applying intrusion detection to SG started roughly from 2009. Klump and Kwiatkowski [12] noticed that it is very important to share the information about cyber risks within the smart grid communications infrastructure, and introduced an IDS mechanism, which was inspired by the federated model, to share the information regarding cyber security risks among smart grid stakeholders, with the purpose of enabling better attack identification and mitigation. Zhang et al. [40] developed a distributed intrusion detection system for smart grids (named SGDIDS) to detect malicious traffic under the power grid network, which consisted of an intelligent module and an analyzing module (AM). To protect multiple layers of SG, multiple AMs can be deployed at each level that utilize the support vector machine (SVM) and artificial immune system (AIS) for detection of possible cyber threats.

Mitchell and Chen [29] then proposed a behavior-rule based intrusion detection system (BRIDS) to help safeguard the critical smart grid applications. They showed that BRIDS could trade false rates according to the requirements, i.e., the detection accuracy is below 6% for random attackers. Lo and Ansari [14] studied false data injection for smart meters and designed a combination sum of energy profiles (CONSUMER) attack, in which intruders can read a lower energy consumption. They further gave a hybrid detection framework to detect anomalous and malicious activities. Pan et al. [32] introduced a systematic approach to automatically build a hybrid IDS to learn patterns from a fusion of synchrophasor measurement data, and power system audit logs for power system. Faisal et al. [8] focused on AMI system and introduced an IDS architecture to monitor smart meter, data concentrator, and AMI headend. They also investigated the feasibility of three data mining algorithms. Genge et al. [10] studied how to design an IDS for smart grid, and they proposed a heuristic approach to decrease the computation time using the column-generation model.

Jokar and Leung [11] introduced HANIDPS, which adopted a model-based intrusion detection mechanism with Q-learning to detect various attacks. Lu et al. [21] targeted on microgrids and provided a model-based anomaly detection and localization strategies to help identify threats in microgrids. Molzahn and Wang [31] introduced an algorithm to extract features and identify attacks by optimizing power flow issues. They also used simulated cases to validate the detection performance. Li *et al.* [15, 18] proposed a concept of intrusion sensitivity based on the observation that personalized IDS nodes may provide different levels of sensitivity in detecting particular intrusions. They then introduced an intrusion sensitivity-based trust management model for CIDNs by assigning the value in an automatic way [16]. They also studied how to apply *intrusion sensitivity* for aggregating alarms and defending against pollution attacks, in

which a group of malicious peers collaborate together by providing false alarm rankings [17]. Other similar work can refer to [1, 13, 30, 33, 35, 38, 39].

Currently, with the increase in grid size and scale, SG needs more resources than traditional electronic grid. Due to this, many approaches start using cloud computing to enhance the performance. A cloud can be used to deliver the on-demand computing power, storage and applications. Hasan and Mouftah [34] identified that smart meters would be one major target by cyber criminals, and a proper solution should balance many factors such as costs, system complexity, and response time. Based on this idea, they designed a cloud-centric collaborative security service architecture for protecting SG, especially the AMI traffic. They also introduced a placement scheme that develops a quadratic assignment problem in order to reduce latency. Anderson et al. [2] focused on the wide area monitoring and control, and found it is difficult to share data in a secure, scalable and cost-effective way. They proposed GridCloud, which is an open-source platform for real-time data collection and sharing in SG. This platform uses commercial cloud tools to reduce costs, adopts cryptographic methods to protect sensitive data, and overcomes failures via software-based redundancy.

Cloud-based platform can ease the burden of computing resources and data storage. However, in modern SG, with the size and scale complexity, communication delay is inevitable between the cloud and the deployed CIDS. The decision latency in SG is extremely sensitive, i.e., a fire might be caused without timely detection of malicious smart meters. Therefore, there is a need for designing a mechanism to further enhance the performance of DIDS / CIDS in SG, especially for AMI and SCADA systems.

3 Background

3.1 Smart Grid

As compared with the traditional electrical grid, SG is developed based on the adoption of communication networking capabilities in order to improve the process of data exchange and automated management in power systems. It is believed to provide much flexibility, resilience, scalability, cost-effectiveness and sustainability. Figure 1 shows the high-level architecture of smart grids including three main layers:

- **Physical Power Layer.** It contains the most important physical parts like power generation, transmission, and distribution. The power generation is mainly performed in power plants, and then power will be delivered from the plants to substations, and finally, delivered from substations to the consumers.
- **Application Layer.** It contains all the services provided to the customers like automated metering. There are various entities including data center, service provider, policy makers, regulation authorities, enterprises, and household, etc.

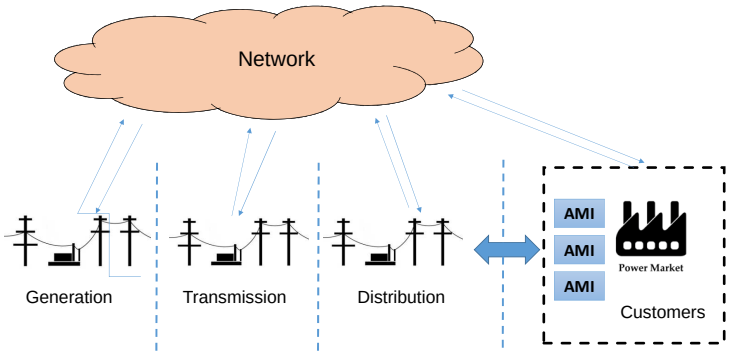

Fig. 1. An overview of Smart Grid architecture.

– **Transport Control Layer.** It contains some major parts to help control how to transmit power. In modern SG, a high speed communication network is usually implemented to ensure the data collection and to handle the interaction and communication among various entities.

In SG, advanced metering infrastructure (AMI) and SCADA systems are very critical. In particular, AMI offers all necessary operations for the bidirectional data exchange between the main power distribution and the customers. It often has three major components [35]: *smart meters* that are used to monitor the power consumption, *data collectors* that are used to store relevant information, and *AMI headend* that acts as a central point to handle the decision based on the stored information. On the other hand, SCADA systems are responsible for monitoring and handling the commands send or received by the logic controllers.

3.2 Collaborative Intrusion Detection

Traditionally, an IDS aims to identify any potential incidents in a computer system or network. An intrusion can be regarded as any events that compromise the pre-defined computer security policies, acceptable use policies, or standard security practices [36]. Based on the deployed location, there could be different types of IDSs such as network-based IDS, host-based IDS, and wireless-based IDS. When detecting a malicious event, an IDS can record the related information and generate alerts to inform security managers.

While a conventional IDS has no information about its protected environment, making it hard to detect complicated and advanced attacks like distributed denial-of-service (DDoS) attack. To improve the detection performance, distributed / collaborative intrusion detection has been developed, which allows a set of detectors exchanging required information [13, 19]. A typical example is the exchange of alarms to decide whether there is a DoS attack.

Figure 2 depicts the typical architecture of collaborative intrusion detection systems, in which IDS nodes can communicate with each other and exchange

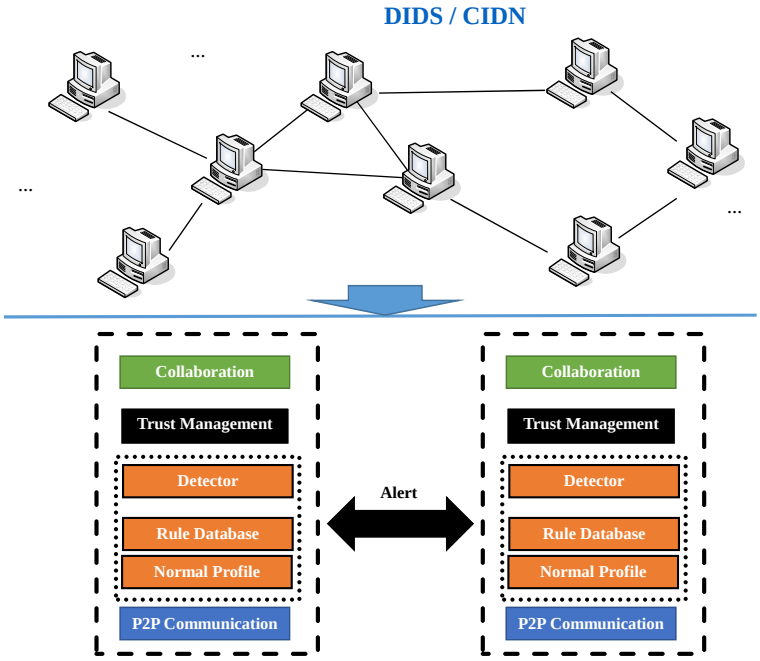

Fig. 2. The typical architecture of collaborative intrusion detection systems.

information. There are several key components in one node: collaboration component, trust management component, IDS component with a detector, a rule database and a normal profile, and P2P communication component.

- **IDS component.** This is the basic part that is responsible for detecting any signs of intrusions by monitoring the computer systems or networks. Various detection methods can be applied here like rule-based and anomaly-based detection.
- **Collaboration component.** This is one main component, which aims to assist a node to communicate with another node, i.e., requesting interested information or sending back required data. To establish a trust management mechanism against insider attacks, this component can also be used to send or receive relevant information, like challenge-based CIDNs [18, 19, 27].
- **Trust management component**. Modern CIDSs often adopt such component to defend against insider attacks, in which an insider malicious node has much more resources than an external node to compromise the protected systems or networks.
- **P2P communication component.** This part is used to keep connection with nearby nodes and offer physical network organization and management.

4 Our Proposed Fog-based CIDS Framework

For the sake of the increasing size of modern smart grid, real-time detection has become much more difficult and critical. Targeted on this issue, in this work, we introduce a fog-based CIDS framework that can further improve the detection performance and reduce the latency caused by the large communication devices and the significant amount of traffic. For instance, the computing burden of an IDS would be at least linear to the size of an incoming payload [22].

The main idea is to use fog computing to reduce the detection delay. Technically, fog computing is relevant to cloud computing, which offers the computing resources and various services to the edge of the network or system. In the literature, it is very close to the term of edge computing. It is believed that edge computing focuses more on the things side, while fog computing puts more emphasis on the infrastructure side [3]. The main feature of fog computing is its proximity to end users, the dense geographical distribution and mobility. For example, fog services are performed nearby the network edge or event end devices, aiming to reduce service latency and improve service quality. Any device with computing, storage, and network connectivity can be a fog node [37].

The idea of using fog computing to improve CIDS in SG is not new, but there are few studies on investigating its effectiveness. In the literature, Chekired et al. [4] provided a hierarchical and distributed intrusion detection system (HD-IDS), which adopted fog computing to secure three levels: home area network, residential area network, and Fog operation center network. Their work focused mainly on the detection of false data injection attack at AMI. Differently, our work emphasizes more on how much detection efficiency of CIDSs could be achieved under fog computing in a SG environment.

The framework is depicted in Figure 3, which involves the SG environment, CIDS, Fog devices, and a cloud. On the whole, it can be roughly considered as four layers.

- **Cloud layer.** This layer provides on-demand computing resources and services, which can be acted as central station to help data storage and analysis.
- **Fog layer.** This layer offers the capability of making decisions nearby the device (the edge of the computer networks), which is more efficient than handling events at central cloud. This layer contains a set of fog devices that provide computing resources and services. Data can be handled based on geographical location without being delivered to the cloud layer.
- **CIDS layer.** This layer provides threat monitoring, detection, and diagnosis. To ensure the detection performance, an IDS node has to exchange information with other nodes like alerts. Detection approaches could be rule-based and anomaly-based. In SG, an IDS can be deployed at any nodes that need protection. Various machine learning algorithms can be applied as well [23–25].
- **SG layer.** This layer contains the major component of SG, from the power generation to power transmission and distribution.

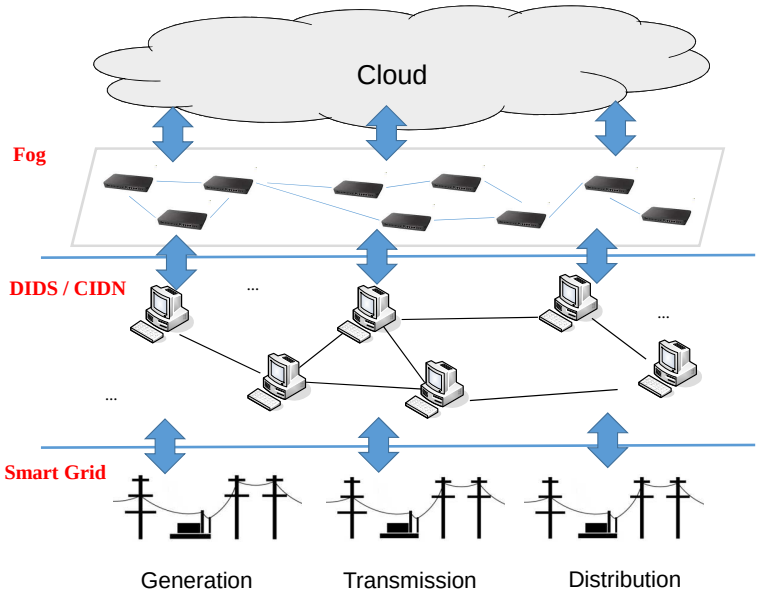

Fig. 3. The typical architecture of collaborative intrusion detection systems.

In the era of IoT, the data volumes could be large, and the following strategies from Cisco can be used to decide sending different types of data to the cloud or fog devices [9].

- The most time-sensitive data should be sent to fog devices for processing, i.e., data should be handled by the fog node closest to where the data come from.
- Data that can afford latency like seconds or minutes can be forwarded to an aggregation node for processing. In SG, the aggregation node should also be close to the data source.
- Data that is not time-sensitive can be delivered to the cloud for traditional processing, like long-term storage. In addition, various fog devices can send their summarized grid data to the cloud for analysis and storage.

5 Evaluation

To explore the performance of our framework, we perform an experiment in collaboration with a grid service provider (in South China) and an IT organization (in South China). The experimental environment is shown in Figure 4. The power grid was constructed based on simulators like GridLAB-D Simulation[3]. The CIDS environment contains a total of 21 nodes, and there are 32 fog devices.

[3] `https://www.gridlabd.org`

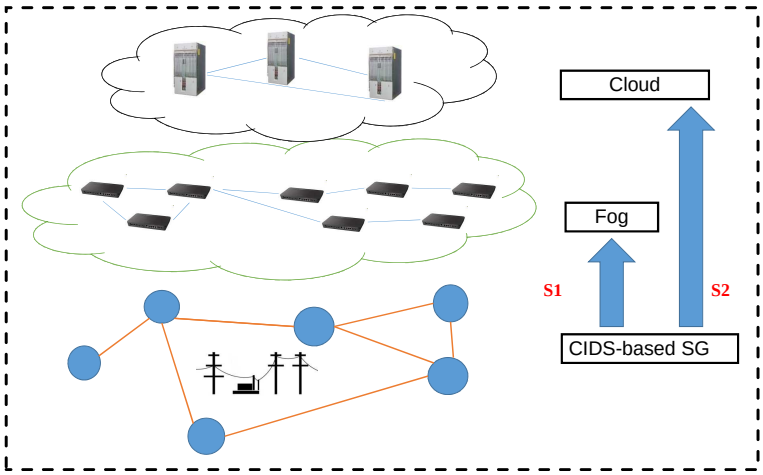

Fig. 4. The experimental environment with two scenarios. S1 means the data will be handled by fog devices, and S2 means the data will be forwarded to cloud for processing.

5.1 Experimental Conditions

As a study, this work mainly focuses on one question: that is, to what degree the CIDS performance can be improved with the use of fog computing. As shown in Figure 4, the following two major scenarios are considered:

- 1) ***S1***: the data will be handled by the fog devices;
- 2) ***S2***: the data will be delivered to the cloud for processing.

We mainly explore the performance of our framework by measuring the difference between S1 and S2. The following two adversarial conditions are studied:

- **Internal attack.** CIDS is known to be suspicious to insider attacks. In SG, collaborated nodes have to exchange information with only trusted partner nodes. To mitigate this issue, we need to deploy trust mechanisms. In this condition, we take challenge-based trust mechanism [19] as a study, which measures the reputation by sending out a kind of message called challenge. For investigation, we take betrayal attack as a case, where a normal node suddenly becomes malicious.
- **External attack.** The main advantage provided by collaborative intrusion detection is the capability of exchanging information like alerts, which can help improve the detection accuracy of complex external attacks. In this condition, we take flooding attack as a study to learn the performance difference between S1 and S2.

For the challenge-based trust mechanism, we adopted the below equation to compute the reputation of a CIDS node. The initial threshold is set as 0.8 based on [19].

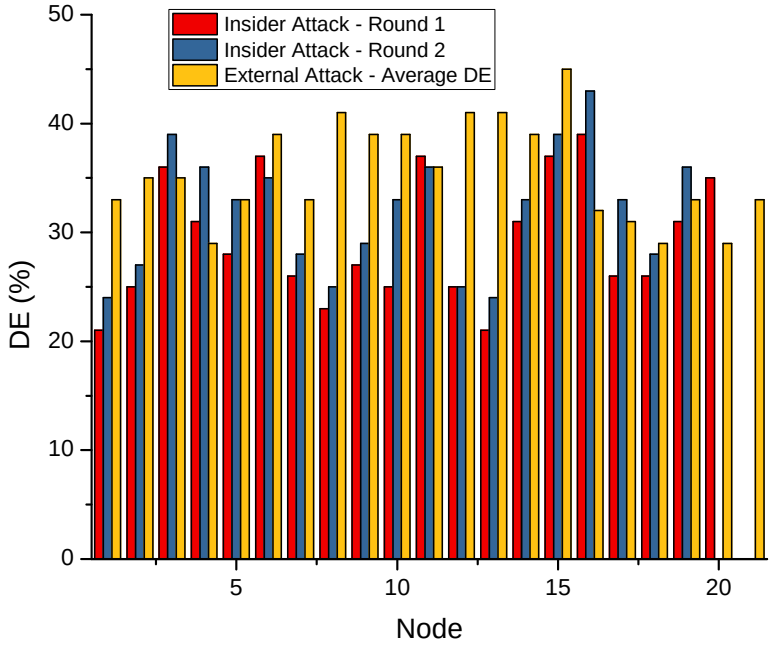

Fig. 5. The detection efficiency (DE) for insider attack under two rounds and external attack: Round 1 only randomly selected one malicious nodes while Round 2 randomly selected two malicious nodes.

$$T_i^j = \left(\frac{\sum_{k=0}^{n} F_k^{j,i} \lambda^{tk}}{\sum_{k=0}^{n} \lambda^{tk}} - T_s\right)(1-x)^d + T_s \tag{1}$$

where $F_k^{j,i}$ means the satisfaction level regarding the k^{th} feedback, and n means the overall feedback number. λ means the forgetting factor that gives more emphasis on the recent feedback. x represents the percent of of "unknown" answers during a period, and d is used to control the severity of punishment to "unknown" answers. More details can be referred to the previous work [18, 19].

5.2 Experimental Results

Insider attack condition. In this study, we launched a betrayal attack by randomly selecting one CIDS node to be malicious. The malicious node can spread malware to other nodes, which could be identified by IDS rules. Our purpose is to investigate the time efficiency between S1 and S2 among the remaining nodes.

External attack condition. In this study, we launched a flooding attack via a traffic generator (https://github.com/Markus-Go/bonesi), where the malicious traffic can be detected by the deployed IDSs. To confirm the situation, IDS nodes

have to exchange the alerts and make a decision. The purpose here is to exploit the time efficiency between S1 and S2.

Results and analysis. To measure the detection performance between S1 and S2, we use the below metric of detection efficiency (DE).

$$DE = \frac{T_{s2} - T_{s1}}{T_{s2}} \tag{2}$$

where T_{s1} means the time consumption under S1 and T_{s2} means the time consumption under S2. The results of detection efficiency are shown in Figure 5.

- **Insider attacks.** We totally performed two rounds of betrayal attacks: we randomly selected one CIDS node as malicious in the first round, and selected two as malicious in the second round. The experiments were repeated five times for each round. The results show that the use of fog devices can help improve the detection efficiency ranged from 21% to 39% and from 24% to 43%, under Round 1 and Round 2, respectively.

  The detection efficiency depends on the geographical location among the CIDS nodes, fog devices and the cloud. Generally, a closer fog device can provide better efficiency. Further, it is found that the improved performance is roughly more visible under Round 2 than Round 1. This is because fog devices can help quickly identify all malicious nodes, while there would be much more delay caused by delivering information to the cloud for analysis and decision.

- **External attacks.** We repeated this experiment five times and Figure 5 shows the average DE value for different CIDS nodes. It is visible that with the help of fog devices, CIDS nodes can detect such flooding attack more quickly than sending information to the cloud. Similar to the insider attack detection, the values of DE varied with geographical distance among the CIDS nodes, fog devices and the cloud, in the range from 29% to 45%. The CIDS node that is closer to a fog device can have a better DE value.

The above results show that the detection efficiency is much better under S1 than S2. In other words, our results demonstrate the positive impact by using fog devices to improve the detection efficiency of CIDSs.

5.3 Validation

To validate the results, we constructed another CIDS environment with a total of 50 nodes and 35 fog devices. We performed the same attacks and the results are shown in Figure 6.

- **Insider attacks.** Similar to the previous experiment, we had two rounds of betrayal attacks: we randomly selected one and two CIDS node as malicious in each round. We repeated experiments five times for each round.

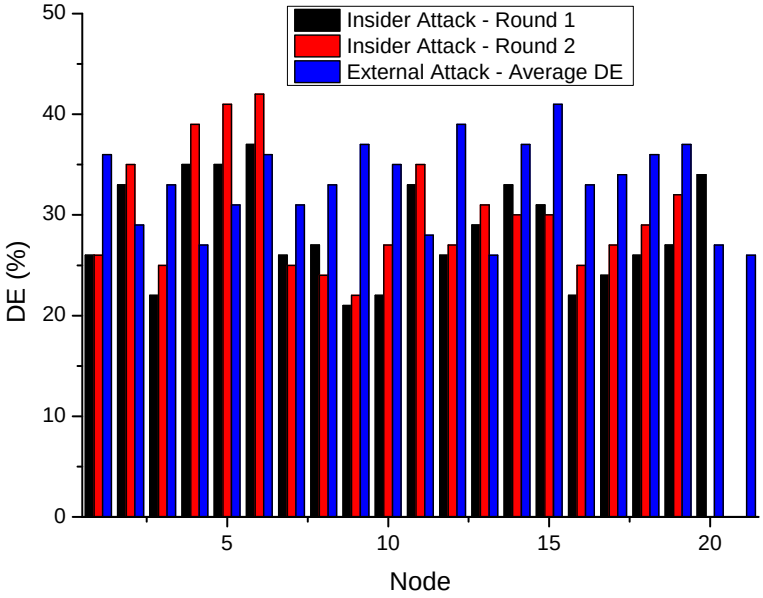

Fig. 6. The detection efficiency (DE) for insider attack under two rounds and external attack: Round 1 only randomly selected one malicious nodes while Round 2 randomly selected two malicious nodes.

The results show that the use of fog devices can help improve the detection efficiency ranged from 21% to 37% and from 24% to 42%, under Round 1 and Round 2, respectively.

– **External attacks.** We repeated this experiment five times and the results indicate that CIDS nodes can detect attacks faster with fog devices than forwarding the information to the cloud, in the range from 26% to 41%.

On the whole, the results validate the effectiveness of our approach. The improved efficiency can vary from 21% to 42% based on the attacking scenarios.

6 Challenges and Discussion

Our study demonstrates that fog computing can be used to enhance the performance of CIDS by alleviating the response time, which is very important for SG. However, SG components like AMI and SCADA systems are still the major target for cyber attackers. There are many security challenges needed to be considered.

– **Various cyber-attacks.** In this work, we mainly consider the improved CIDS performance by adopting the fog computing. Due to the vulnerabilities

in SG, many more efforts are needed to protect such environment from cyber-attacks. For example, there is a need to protect unauthorized access to the infrastructure, and safeguard the privacy of data. Without timely detection, SG attacks can lead to a devastating impact on the critical infrastructures relying on power supply. Further, how to maintain the data integrity and privacy has become a major concern from the customers.

- **Environmental security.** This factor can help control the impact of potential damage on the infrastructures due to any of natural or human-caused environmental hazards. As an example, the hurricane sandy in US caused a loss of $70 billion, and a disruption in power supply for over 8 million customers in 2012. In addition, how to organize the fog devices could depend heavily on the environmental conditions.
- **Operational security.** Due to the grid size, the SG critical infrastructures and relevant operations would become more complex. Operational security thus becomes a challenge, which is relevant to infrastructural installations, control procedures, operational reliability and resiliency, system intelligence, regular checking process and maintenance plan, etc. All these aim to achieve a more robust SG environment.
- **CIDS detection capability.** Although the use of cloud and fog computing can help improve the efficiency of CIDSs, it is still a challenge to develop an effective detector for SG. This is because most commercial IDSs do not have specialized rules to build a normal profile for SCADA systems. That is, a CIDS node has to be tuned based on the particular SG environments and requirements.
- **CIDS security.** Collaborative intrusion detection is an essential security solution for protecting SG; however, CIDS has its inherent limitations. For instance, due to the distributed nature, CIDS is vulnerable to insider attacks. To mitigate such issue, appropriate trust mechanisms should be established to protect CIDS, as well as SG environments. For example, the challenge-based trust mechanism can be used to evaluate the reputation of another nodes according to its feedback [19]. Recently, blockchain technology also received much attention [20, 28]. This is an interesting and important topic for future investigation.
- **Limitations of fog computing.** Although fog computing can complement cloud environment, it also suffers from many limitations. For instance, fog devices have to use global storage that may result in the complexity of data management. Data schedule is a major concern, by moving data between the central cloud and end users. In addition, fog computing cannot solve the traditional trust and authentication issues. In practical implementation, predefined encryption schemes and security policies may also cause difficulty in exchanging data among fog devices.

7 Conclusion

With the increasing adoption of ICT and cloud computing in smart grid, it is very critical to reduce the detection latency caused by the distance between

the cloud and smart grid. In this work, we focus on improving the detection efficiency and propose a fog-based CIDS framework to help make a decision near the CIDS node. In the evaluation, we examine the performance of our framework under both internal and external attacks. The results demonstrate that our framework can greatly reduce the latency and enhance the detection efficiency, i.e., enhancing the detection efficiency ranged from 21% to 39% and from 24% to 43% for two internal attack scenarios; and from 29% to 45% for external attack scenario.

Acknowledgments. This work was partially supported by National Natural Science Foundation of China (No. 61472091).

References

1. M.Q. Ali, R. Yousefian, E. Al-Shaer, S. Kamalasadan, Q. Zhu: Two-tier data-driven intrusion detection for automatic generation control in smart grid. In: Proceedings of CNS, pp. 292-300, 2014.
2. D. Anderson, T. Gkountouvas, M. Meng, K. Birman, A. Bose, C. Hauser, E. Litvinov, X. Luo, Q. Zhang: GridCloud: Infrastructure for Cloud-Based Wide Area Monitoring of Bulk Electric Power Grids. IEEE Trans. Smart Grid 10(2): 2170-2179, 2019.
3. F. Bonomi, R.A. Milito, J. Zhu, S. Addepalli: Fog computing and its role in the internet of things. MCC@SIGCOMM 2012: 13-16.
4. D. A. Chekired, L. Khoukhi, H.T. Mouftah: Fog-Based Distributed Intrusion Detection System Against False Metering Attacks in Smart Grid. ICC 2019: 1-6.
5. X. Ma, Smart Grid. Online Available: `https://www.cse.wustl.edu/~jain/cse574-10/ftp/grid/index.html`
6. US Gas Pipeline Hit by Cyber Attack. April 2018. Available online: `https://www.infosecurity-magazine.com/news/us-gas-pipelines-hit-by-cyberattack/`
7. Europa EU - Smart Grid Security: Annex II. Security aspects of the smart grid. April 2012. Available online: `https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/`
8. M.A. Faisal, Z. Aung, J.R. Williams, A. Sanchez: Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study. IEEE Systems Journal 9(1), pp. 31-44, 2015.
9. Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are, White Paper, 2015. Online: `https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf`
10. Bela Genge, Piroska Haller, Cristian-Dragos Dumitru, Calin Enachescu: Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids. IEEE Trans. Smart Grid 8(5), pp. 2440-2451, 2017.
11. P. Jokar, V.C.M. Leung: Intrusion Detection and Prevention for ZigBee-Based Home Area Networks in Smart Grids. IEEE Trans. Smart Grid 9(3), pp. 1800-1811, 2018.
12. R. Klump, M. Kwiatkowski: Distributed IP Watchlist Generation for Intrusion Detection in the Electrical Smart Grid. Critical Infrastructure Protection 2010: 113-126.

13. X. Liu, P. Zhu, Y. Zhang, K. Chen, A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure. IEEE Trans. Smart Grid 6(5): 2435-2443 (2015).
14. C.-H. Lo, N. Ansari: CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid. IEEE Trans. Emerging Topics Comput. 1(1), pp. 33-44, 2013.
15. Li, W., Meng, Y., Kwok, L.-F.: Enhancing Trust Evaluation Using Intrusion Sensitivity in Collaborative Intrusion Detection Networks: Feasibility and Challenges. In: Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS), pp. 518–522, IEEE (2013)
16. Li, W., Meng, Y., Kwok, L.-F.: Design of Intrusion Sensitivity-Based Trust Management Model for Collaborative Intrusion Detection Networks. In: Proceedings of the 8th IFIP WG 11.11 International Conference on Trust Management (IFIPTM), Springer, pp. 61-76 (2014)
17. Li, W., Meng, W.: Enhancing Collaborative Intrusion Detection Networks Using Intrusion Sensitivity in Detecting Pollution Attacks. Information and Computer Security, vol. 24, no. 3, pp. 265-276 (2016)
18. Li, W., Meng, W., Kwok, L.-F., Ip, H.H.S.: Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. Journal of Network and Computer Applications 77, pp. 135-145 (2017)
19. Li, W., Meng, W., Kwok, L.-F., Ip, H.H.S.: Developing advanced fingerprint attacks on challenge-based collaborative intrusion detection networks. Cluster Computing 21(1): 299-310, 2018.
20. Li, W., Tug, S., Meng, W., Wang, Y.: Designing Collaborative Blockchained Signature-based Intrusion Detection in IoT environments. Future Generation Computer Systems, vol. 96, pp. 481-489 (2019)
21. L.-Y. Lu, H.J. Liu, H. Zhu, C.-C. Chu: Intrusion Detection in Distributed Frequency Control of Isolated Microgrids. IEEE Trans. Smart Grid 10(6), pp. 6502-6515, 2019.
22. Y. Meng, W. Li and L.-F. Kwok. Towards Adaptive Character Frequency-based Exclusive Signature Matching Scheme and its Applications in Distributed Intrusion Detection. Computer Networks, vol. 57, no. 17, pp. 3630-3640, 2013.
23. Y. Meng, L.-F. Kwok. Enhancing False Alarm Reduction Using Voted Ensemble Selection in Intrusion Detection. International Journal of Computational Intelligence Systems, vol. 6, no. 4, pp. 626-638, May 2013.
24. Y. Meng, L.-F. Kwok. Adaptive Blacklist-based Packet Filter with A Statistic-based Approach in Network Intrusion Detection. Journal of Network and Computer Applications, vol. 39, pp. 83-92, 2014.
25. Y. Meng, L.-F. Kwok. Adaptive Non-Critical Alarm Reduction Using Hash-based Contextual Signatures in Intrusion Detection. Computer Communications, vol. 38, pp. 50-59, 2014.
26. W. Meng, W. Li, L.F. Kwok, Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments. IEEE Trans. Network and Service Management 14(1): 233-245, 2017.
27. W. Meng, W. Li, L.T. Yang, P. Li. Enhancing Challenge-based Collaborative Intrusion Detection Networks Against Insider Attacks using Blockchain. International Journal of Information Security, Springer (2019) [https://doi.org/10.1007/s10207-019-00462-x]

28. W. Meng, W. Li, L. Zhu. Enhancing Medical Smartphone Networks via Blockchain-based Trust Management against Insider Attacks. IEEE Transactions on Engineering Management, IEEE, In Press.
29. R. Mitchell, I.-R. Chen: Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications. IEEE Trans. Smart Grid 4(3), pp. 1254-1263, 2013.
30. N.B. Mohammadi, J.V. Misic, H. Khazaei, V.B. Misic: An intrusion detection system for smart grid neighborhood area network. In Proceedings of ICC, pp. 4125-4130, 2014.
31. D.K. Molzahn, J. Wang: Detection and Characterization of Intrusions to Network Parameter Data in Electric Power Systems. IEEE Trans. Smart Grid 10(4), pp. 3919-3928, 2019.
32. S. Pan, T.H. Morris, U. Adhikari: Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. IEEE Trans. Smart Grid 6(6), pp. 3104-3113, 2015.
33. A. Patel, H. Alhussian, J.M. Pedersen, B. Bounabat, J.C. Junior, S.K. Katsikas: A nifty collaborative intrusion detection and prevention architecture for Smart Grid ecosystems. Computers & Security 64: 92-109, 2017.
34. M.M. Hasan, H.T. Mouftah: Cloud-Centric Collaborative Security Service Placement for Advanced Metering Infrastructures. IEEE Trans. Smart Grid 10(2): 1339-1348, 2019.
35. P.I. Radoglou-Grammatikis, P.G. Sarigiannidis, Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. IEEE Access 7: 46595-46620, 2019.
36. K. Scarfone and P. Mell, Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology (NIST), 2007.
37. Y. Wang, W. Meng, W. Li, Z. Liu, Y. Liu, H. Xue. Adaptive Machine Learning-based Alarm Reduction via Edge Computing for Distributed Intrusion Detection Systems. Concurrency and Computation: Practice and Experience, vol. 31, no. 19, 2019.
38. W. Wang, Y. Shang, Y. He, Y. Li, J. Liu, BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors, Information Sciences, volume 511, no. 2, pp. 284-296 (2020). DOI: https://doi.org/10.1016/j.ins.2019.09.024
39. G. Xu, W. Wang, L. Jiao, X. Li, K. Liang, X. Zheng, W. Lian, H. Xian, H. Gao, SoProtector: Safeguard Privacy for Native SO Files in Evolving Mobile IoT Applications, IEEE Internet of Things Journal (early access), 30 September 2019, pp. 1-1. DOI: 10.1109/JIOT.2019.2944006.
40. Y. Zhang, L. Wang, W. Sun, R.C. Green II, M. Alam: Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. IEEE Trans. Smart Grid 2(4): 796-808, 2011.