TPRou: A Privacy-Preserving Routing for Payment Channel Networks

Zijian Bao[1], Qinghao Wang[1,2], Yongxin Zhang[2,4], Hong Lei[1,3(✉)], and Wenbo Shi[2]

[1] Hainan Nanhai Cloud Holding Co., Ltd., Chengmai 571924, China
{zijian,qinghao,leihong}@oxhainan.org
[2] School of Computer Science and Engineering, Northeastern University, Shenyang 110001, China
shiwb@neuq.edu.cn
[3] School of Cyberspace Security, Hainan University, Hainan 570228, China
[4] Oxford-Hainan Blockchain Research Institute, Chengmai 571924, China

Abstract. Although cryptocurrencies have achieved great success in recent years, building large-scale fast payments is still a challenge. Payment channel networks (PCNs), as a practical solution to resolve this problem, can realize numerous off-chain settlements of transactions without heavy on-chain operations. The core of PCN is a routing scheme that discovers transaction paths with sufficient funds between the sender and receiver. However, the leakage of private information (*e.g.,* the identity of senders and receivers, transaction value) becomes one tricky issue. In this work, we proposed TPRou, a privacy-preserving PCN routing scheme leveraging trusted execution environments (TEEs), which can provide broader privacy guarantees than the state-of-the-art routing schemes. TPRou constructs redundant paths with different receivers to hide the identity of the receiver. Moreover, TPRou introduces a novel identity information transfer scheme, called an *encrypted identity chain*, to hide the identity of the sender and the receiver from the intermediate nodes in the payment path. Based on security analysis and performance evaluation, our result demonstrates that TPRou is able to achieve privacy-preserving payment with minimal overhead.

Keywords: Payment channel networks · Routing · Trusted execution environment (TEE) · Intel software guard extensions (SGX) · Blockchain

1 Introduction

Although cryptocurrencies have been widely concerned, their application is limited by pool scalability. For example, limited by the consensus mechanism

This study is supported by Finance Science and Technology Project in Hainan Province (No. ZDKJ2020009), the National Natural Science Foundation of China (Nos. 62072093 and U1708262), the Fundamental Research Funds for the Central Universities (No. N172304023).

E. Bertino et al. (Eds.): ESORICS 2021, LNCS 12973, pp. 764–769, 2021.
https://doi.org/10.1007/978-3-030-88428-4

ensuring the data consistency in an untrusted environment, Bitcoin can only process 7 transactions per second(tps), demonstrating a huge gap with the real scenarios of a payment system (*e.g.*, Visa handles 1500 tps).

The payment channel is a promising proposal to improve cryptocurrency scalability. It is a layer-two solution, combining on-chain and off-chain operation, to reduce blockchain burden while keeping the normal payment function. First, two users build a payment channel with a transaction to lock money on the chain. Then, they can reallocate this locked money off-chain fastly. Finally, one can send a transaction to close the channel with the latest money allocation plan.

Payment channels can be linked together to form a payment channel network (PCN), such as Lightning Network in Bitcoin. The core of PCN is a routing scheme that discovers payment paths between the sender and receiver. The existing PCN routing schemes can be classified into *non-landmark* and *landmark-based* schemes, according to the participation of noted nodes named *landmarks*. In the *non-landmark* schemes, the user itself is responsible for routing, introducing a heavy overhead of computation, storage and communication. The *landmark-based* schemes are more popular because it frees the users from these burdens. However, the landmark will acquire sensitive information such as the *transaction value and the identity of the senders and receivers*.

To tackle this problem, Moreno-Sanchez *et al.* [2] employ secret sharing and multi-party secure computation technologies to hinder transaction value. Moreover, SpeedyMurmurs [3] makes a further effort by providing higher overall performance while protecting the identity of the receiver. However, SpeedyMurmurs just split the value of the transaction without further protecting it, which raises the risk of privacy leakage. Resorting to *landmarks* to implement PCN routing while considering identity and transaction value privacy is a problem worth studying.

In this work, we present TPRou, a landmark-based routing scheme, finding the feasible paths and enable multi-hop payment with a manner of privacy-aware. It can provide broader privacy guarantees than the state-of-the-art routing schemes. Specifically, TPRou enforces the confidential data of routing in the trusted execution environment (TEE) controlled by the landmark node to prevent privacy leakage. To hide the receiver, TPRou constructs redundant paths with different receivers in the TEE. Moreover, TPRou introduces a novel identity information transfer scheme, called an *encrypted identity chain*, which is compatible with the multi-hop payment. It is capable of hiding the identity of the sender and the receiver from the intermediate nodes in the payment path. Finally, the security analysis and performance evaluation show that TPRou is able to achieve privacy-preserving payment with minimal overhead.

2 Our Design

We describe the key ideas of TPRou, including the *preparation*, *path building* and *executing payment* stages. The work flow is shown in Fig. 1. TPRou contains following entities: users (*e.g.*, senders, receivers and intermediate users) and

TEE-based landmarks (TLs). Since our scheme uses Intel SGX as the instance of TEE, we will default that TEE supports the features provided by SGX [1].

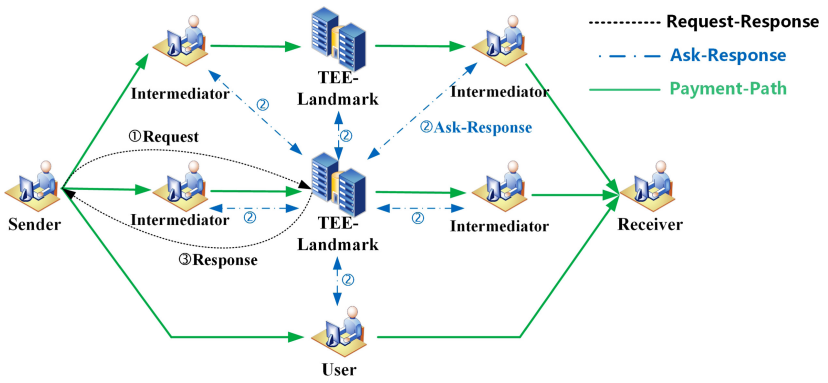


Fig. 1. An illustrative example of the path building stage of TPRou: Black lines show communications between the senders and TLs. Blue lines show communications between intermediate users and TLs. We consider a payment from a sender to a receiver. ① A sender sends a request to TL for a path to pay. ② The TL searches the intermediate users and asks them if they can meet the request of the sender. ③ The TL gives the sender a response including the feasible path.

Preparation Stage: In this stage, preparations are mainly carried out, such as TL nodes' joining the payment channel network, broadcasting their identities and related public keys to the entire network, and declaring that they will provide routing services for users. Any node can use remote attestation to authenticate the TL's identity and the code in the TEE to ensure trustworthiness. Moreover, a secure communication channel can be constructed between nodes and TLs. TL maintains a global topology of payment channel routing.

Path Building Stage: The sender sends a multi-hop routing request to the TL (① in Fig. 1). Then, TL constructs multiple payment paths (one is the real path and others are the redundant paths with pseudo receivers) according to the existing topology and verifies whether the path nodes meet the routing conditions, such as routable value and transaction fees (② in Fig. 1). Note that TL executes the breadth first search (BFS) algorithm in the TEE to construct the shortest path from the sender to the receiver. TL needs to record the round number of the enquiry to prove that the TEE owner does not deliberately abandon the path. If an available path is found, TL will enter the next stage. Otherwise, TL will inform the sender that there is no proper path (③ in Fig. 1).

Executing Payment Stage: In this stage, TL mainly informs the sender of path node information (③ in Fig. 1), including node identity and transaction fees. The sender builds a multi-hop payment request based on the above information.

In particular, to ensure the identity privacy of the sender and receiver among the intermediate users, the *encrypted identity chain* is designed. The sender built it with the nodes' public keys in an order from the receiver to the sender. The form of *encrypted identity chain* as follows:

$$CreID_i = \begin{cases} \{ID_{i+2}, CreID_{i+1}\}_{PKi+1}, & i \in [0, n-3] \\ \{ID_n\}_{PKi+1}, & i = n-2 \end{cases}$$

For example, in the path $\{node_{sed}, node_1, node_2, ..., node_{n-2}, node_{rec}\}$, the $node_4$ will receive the $\{ID_5, CreID_{4PK_4}\}$ from $node_3$. The $node_4$ decrypts it with its secret key, obtains ID_5 (*i.e.,* its next hop) and $CreID_4$ (*i.e.,* the content for its next hop).

3 Security Analysis

In this section, we give a brief analysis to show how our scheme can achieve privacy protection. The Table 1 shows the comparison of PCN routing schemes.

Table 1. The comparison of PCN routing schemes

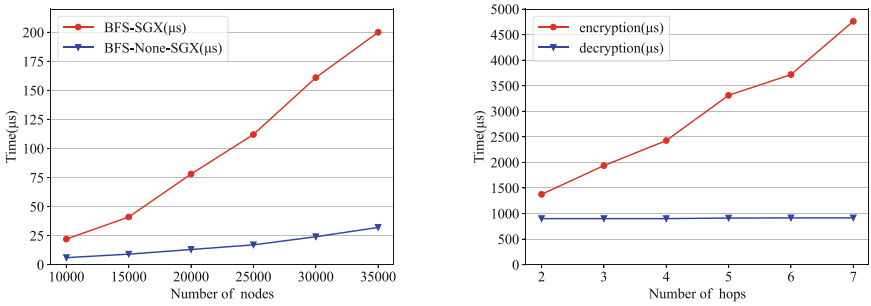
	SilentWhisper[2]	SpeedyMurmurs[3]	Spider[4]	**TPRou**
Types	Landmark	Landmark	Non-Landmark	Landmark
Sender's privacy	●	●	-	●
Receiver's privacy	○	●	-	●
Transaction value privacy	●	◐	○	●

● means that the schemes has the function, while ○ means not. ◐ means the schemes provides limited functionality.

Sender Privacy and Receiver Privacy. We improve the privacy-preserving of PCN routing in two ways. On the one hand, the confusion technique is used to hinder the identity of the receiver from the landmark. When sending a multi-hop payment request to the landmark, the sender sets multiple receivers in the **Path building stage**, so that landmark is impossible to directly determine which node is the real receiver. In previous work [2], the landmark only communicates with nodes in one path, it can easily determine the identity of the receiver. On the other hand, the *encrypted identity chain* is adopted to hinder the identity of the sender and the receiver from intermediate nodes. The next hop is encrypted by the node's public key, and only itself can decrypt it. Intermediate nodes only learn their neighbours (i.e., last hop and next hop) rather than the whole path.

Value Privacy. TPRou achieves value privacy whether the path exists or not. If the path exists, the transaction amount is added to the *encrypted identity chain*, and the remaining nodes cannot decrypt it. Otherwise, the transaction amount is encrypted by the key from TEE, and the TEE platform holder cannot decrypt it. In work [3], the transaction amount is divided into pieces rather than the protection of cryptography technology.

4 Performance Evaluation



(a) Time cost comparisons between SGX and non-SGX environments

(b) Time cost of the *encrypted identity chain* algorithm with different hops

Fig. 2. The results of performance evaluation

To analyze the efficiency of TPRou, we implement our scheme using Intel SGX as the instance of TEE, and evaluate the performance of it. First, we implemented the BFS-based routing algorithm with different numbers of nodes (where 25,000 is similar to the number in Bitcoin's Lightning Network) in the SGX and non-SGX environment. Figure 2(a) shows that the execution time in SGX requires higher overhead, but such overhead is acceptable as several SGX-enabled landmarks that are profit-driven can cover the whole PCN.

Then, we implemented the *encrypted identity chain* algorithm based on the ECC algorithm (note that our scheme is compatible with any signature algorithm supported on any blockchain) and tested the overhead of multiple payments with different hop counts (2 to 7 hops which are the common range of the Lightning Network). Figure 2(b) shows the operation overhead of the sender (encryption) and the intermediate node (decryption). The encryption overhead increases linearly as the number of hops increases. And the decryption overhead is constant because each node only needs to decrypt once. In summary, our scheme is able to achieve privacy-preserving payment with minimal overhead.

5 Conclusion

In this work, we propose TPRou, a privacy-preserving payment channel network routing scheme. Thanks to TEE, the transaction value privacy is protected from the landmarks. To hide payment receivers, TPRou constructs redundant paths with different receivers in the TEE. We design an *encrypted identity chain* to hide transaction information in the payment process. The experiment shows that TPRou achieves privacy protection while maintaining low computation overhead.

References

1. Costan, V., Devadas, S.: Intel SGX explained. IACR Cryptol. ePrint Arch. **2016**(86), 1–118 (2016)
2. Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M.: SilentWhispers: enforcing security and privacy in decentralized credit networks. In: 24th Annual Network and Distributed System Security Symposium, NDSS (2017)
3. Roos, S., Moreno-Sanchez, P., Kate, A., Goldberg, I.: Settling payments fast and private: efficient decentralized routing for path-based transactions. In: 25th Annual Network and Distributed System Security Symposium, NDSS (2018)
4. Sivaraman, V., et al.: High throughput cryptocurrency routing in payment channel networks. In: 17th USENIX Symposium on Networked Systems Design and Implementation, NSDI (2020)

Determining Asset Criticality in Cyber-Physical Smart Grid

Yazeed Alrowaili(✉), Neetesh Saxena, and Pete Burnap

School of Computer Science and Informatics, Cardiff University, Cardiff, UK
{alrowailiyf, saxenan4, burnapp}@Cardiff.ac.uk

Abstract. Cybersecurity threats in smart grids have incredibly increased in the past years, and there is a strong need to protect these critical systems. Moreover, cyber-risk assessment and determining asset criticality are needed to apply the best remediation plan if the system is compromised. Still, due to the heterogeneity between operation technology (OT) and information technology, it is not easy to protect such a system altogether. Hence, the criticality of OT resources should be identified by their characteristics, helping operators understand that different assets can cause additional damage and require further protection or need more vital remediation plans. In this work, we proposed a methodology that can identify and indicates the frequency and impact of an asset in the system to determine its criticality. Moreover, the effectiveness and feasibility of the proposed method are evaluated by a 12-bus power system using the PowerWorld simulator by performing attacks on critical assets such as circuit breakers and evaluated their impact on the physical system. Finally, the test results demonstrate that targeting the most critical assets identified can severely impact the system while targeting the least critical assets is manageable.

Keywords: Smart grid · Cyber risks · Critical assets · Attack impact · OT

1 Introduction: Context and Motivation

Smart grids (SGs) can be classified as one of the many types of critical infrastructure. Moreover, it can monitor the flow of measurement units such as power from generation to consumption and match generation flow in real-time or near real-time by limiting and/or controlling any electrical load [1]. It provides control automation and transmit power from generation plants to transmission lines, distribution substations, and later to the consumers. Furthermore, cybersecurity threats targeting these systems have incredibly increased, and the failure to protect these OT assets will cause a significant impact [2]. According to the research analysis of the cyber-attack on the Ukrainian Power Grid done by E-ISAC and SANS ICS, on Dec. 23, 2015, there was a service outage on three energy companies that affected 225,000 customers for 3–7 h in 103 cities [3]. Moreover, the current focus on protecting such a system is either specified on listing the possible attacks or attack paths that can occur on the system or classifying the criticality of ICS assets from an IT or business perspective [4]. Yet, there is little focus on criticality evaluation based on the damage that can occur after a successful attack on OT assets under physical processes.

E. Bertino et al. (Eds.): ESORICS 2021, LNCS 12973, pp. 770–776, 2021.
https://doi.org/10.1007/978-3-030-88428-4

Contribution. Firstly, we proposed a new method that identifies and determines the criticality of OT assets within the physical system. Secondly, we evaluated the proposed method using the PowerWorld with a 12-bus case by performing attacks on critical assets, such as circuit breakers, and measured their impact on the physical system. Finally, we analysed the damage when the most critical and the least critical assets are zero-day at-tacked, gaining unauthorised access to the system by exploiting software vulnerability [5].

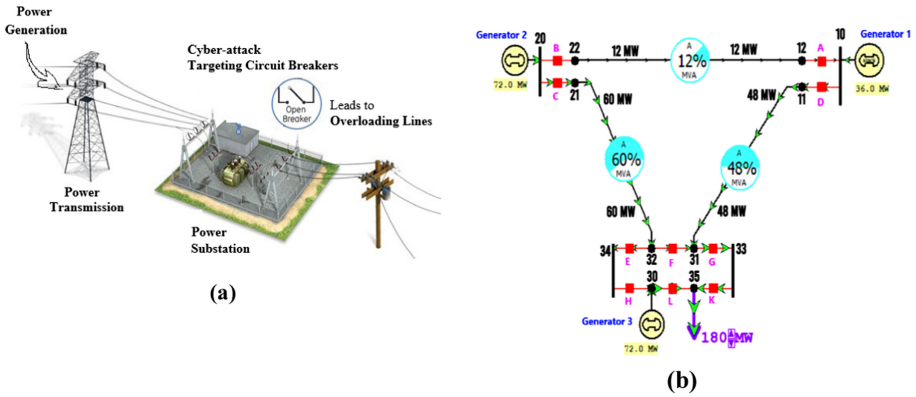


Fig. 1 **(a)** Smart grid substation system model. **(b)** 12-bus power system case normal scenario

2 Related Work

Attacks targeting assets at physical level are challenging to deal with, as evaluating assets criticality in a SG system should be specific to its characteristics. In this direction, Hasan et al. [6] proposed a method to detect and evaluate paths to critical energy delivery system nodes with network heterogeneity. However, the work uses logs and host logs, which mostly exist in IT systems. Corallo et al. [9] proposed a metric to evaluate assets criticality in the context of industry 4.0, aiming to recognise and assess the critical assets in ICS to protect them against cyber threats. However, this work was mainly focused on what impact can occur from a business perspective and quite limited in terms of offering a comprehensive evaluation for assets criticality in OT. Crespo et al. [10] proposed criticality evaluation in power line systems to offer a reliable, fast-maintained process in these systems by performing asset criticality evaluation and use the collected information to update the appropriate maintenance plan. Nevertheless, this work concentrates on assets maintenance strategy and determining its criticality they deal with, and the evaluation was also conducted on limited nodes. Recently, Vallant et al. [7] offer risk assessment methodology by identifying all possible vulnerabilities to cyber secure SG systems. However, the work focuses potential threats and the likelihood of successful attacks only. In order to fill the gaps in identifying asset criticality in OT systems and evaluating cyber risks impact on the physical systems, we not only proposed a method for discovering OT assets with most and least criticality, but also evaluating their impact on smart grid system using PowerWorld simulator.

3 Approach

Our aim is to propose a method that can identify the most critical assets in the physical system and evaluates adverse impact that may occur when the system is compromised.

3.1 System Model and Simulation Scenario

Figure 1(a) presents a power substation system model where an adversary can target critical assets such as circuit breakers or transformers to create physical and/or operational damage to the system. Further, Fig. 1(b) shows a test case of a 12-bus system regularly operated with normal scenario on the Powerworld simulator. Moreover, this case was used to show this study on critical components, and it contains 12 buses, 3 generators, 10 breakers and one load. Furthermore, the focus is identifying the most critical asset (circuit breakers), seen as red squares. When an adversary attacks critical circuit breakers, it will cause all generators to increase their reactive power *(Mvar)*, consequently reducing system reliability and efficiency, making the system to no longer supply load, which can cause a blackout [8].

3.2 Proposed Method

We present the proposed method to determine criticality of each asset in the smart grid system and evaluate their cyber impact using PowerWorld tool. This method can be generalized to other cyber-physical systems considering relevant devices and OT operational impact. Further, identify most and least critical assets (scanning devices and apply our method) and then apply risk assessment methodologies to analyse cyber risks, and evaluate their impact (e.g., simulation) on physical systems. In our scenario, we determine each circuit breaker based on its frequent occurrence in use while supplying power from a *generator* to the load using a specified path. Moreover, this can be applied by identifying all possible P paths that a generator *(i)* uses to transmit the power as per the load requirement, then assess how many times (how frequently) a circuit breaker *(i)* Cb_i is used in all paths. The criticality can be calculated as:

$$\text{Criticality} = Cb_i/P \tag{1}$$

Algorithm1 Calculate Criticality of an Asset in Smart Grid

Input: All paths P for generator *(i)* & Number of frequent uses of Cb_i in all paths.
Output: Criticality score for Cb_i linked to a specified generator.

1: Let **P** denote total number of paths generator *(i)* uses to transmit the power to the load.
2: Let $\mathbf{Cb_i}$ indicate how many times circuit breaker *(i)* has been used in all paths **P**.
3: Applying *Equation (1)* listed above. *(where $0 \leq score \leq 1$)*
4: **if (**Cb_i score is > 0.5 *(meaning that Cb_i has appeared in more than half of paths)*) **then**
5: Declare most critical asset.
6: **else**
7: Declare least critical asset.

Table 1. Shows all possible paths and circuit breakers that existed in each path generator *(1,2,3)* uses to transmit power to load.

ID		A	B	C	D	E	F	G	H	L	K
Gen1	Path 1	✓	✓	✓			✓	✓			✓
	Path 2				✓			✓			✓
	Path 3				✓	✓	✓		✓	✓	
Gen2	Path 1	✓	✓		✓			✓			✓
	Path 2			✓		✓			✓	✓	
	Path 3			✓			✓	✓			✓
Gen3	Path 1									✓	
	Path 2					✓	✓	✓	✓		✓

Table 1 shows the frequent use of circuit breakers in all paths for *generators 1, 2, and 3*. Moreover, applying *Algorithm 1* in all generators with the giving data will indicate that circuit breakers ***(D, F, G, K)*** are considered the critical asset for ***generator 1***, and for ***generator 2*** are ***(C, G, K)***. Moreover, circuit breaker ***(L)*** is considered critical as the other breakers since it is the only breaker used in a specific path with ***generator 3***. Therefore, the most critical circuit breakers in this 12-bus system test case are ***(D, F, G, C, K, L)***.

4 Experimental Results and Evaluation

This section shows an evaluation of our methodology when targeting the system's critical assets with zero-day attack and monitor generators reactive power *(Mvar)* for any changes.

4.1 System Operations Under No Attack Scenario

Table 2 shows generators information under a normal scenario, indicating that the measurements of *(Gen MW)* and *(Gen Mvar)* are normal and the system is under control, as shown in Fig. 1. We have kept *Gen MW* constant for our experiments and observing *Gen Mvar* values when targeting most vs. least critical assets in the system.

Table 2. Generators measurements on normal scenario

ID	Number of bus	Name of bus	Gen *MW*	Gen *Mvar*
1	10	10	36.00	1.23
2	20	20	72.00	1.88
3	30	30	72.00	2.97

4.2 System Operations Under Attack Scenario

Table 3 shows generators measurements when targeting the most critical circuit breakers [(F, L), C, D]. It can be seen that compromising the most critical breakers made the reactive power *(Gen Mvar)* for related generators increasing highly, which can cause overloaded transmission lines and/or overheating, as demonstrated in Fig. 2. For example, opening F and L circuit breakers (for generator 3) increases *Gen Mvar* (44.13 and 12.81) for generator 1 and 2, respectively, while it is further decreased for generator 3 (2.74) as compared to original *Gen Mvar* values from Table 2. As a result, line 10–20 and 10–33 are overloaded with 144% and 183%, respectively. This is true for other two cases as reflected in Fig. 2, when a circuit breaker C and D are opened in each case, which resulted into overloading lines 10–33 and 20–34 with 108%.

Table 3. Generator's measurements when targeting most critical circuit breaker (D), *(C) or (F, L)*

Gen ID	Gen *MW for (F, L)*	Gen *Mvar for (F, L)*	Gen *MW for (C)*	Gen *Mvar for (C)*	Gen *MW for (D)*	Gen *Mvar for (D)*
1	36.00	44.13	36.00	8.47	36.00	0.65
2	72.00	12.81	72.00	1.60	72.00	6.51
3	72.00	2.74	72.00	5.83	72.00	5.88

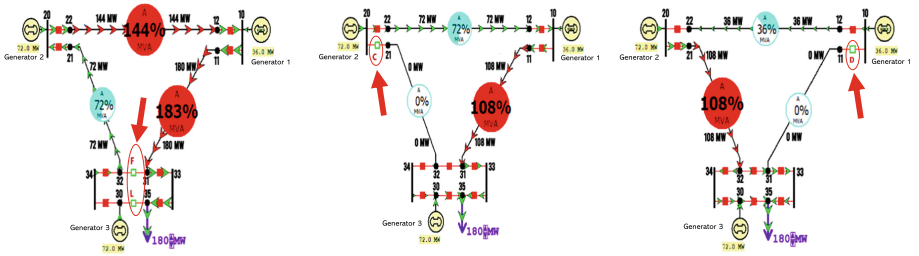


Fig. 2 Attacker compromises most circuit breakers in respective order *(F, L), (C), and (D)*

Further, Table 4 shows generators' measurements when targeting some of the least critical circuit breakers. Moreover, it can be seen that compromising the least critical breakers made the reactive power *(Gen Mvar)* for relevant generators increase slightly. Yet, it can be seen in Fig. 3 that the system is under control, and there are no threats or overload in transmission lines. As we can observe, line 10–20 is disconnected after opening A and B circuit breakers, whereas the lines 20–34 and 10–33 are with 72% and 36% capacity, respectively, once H circuit breaker is further opened.

Table 4. Generator's measurements when targeting the least critical circuit breakers *(A, B, H)*

Gen ID	Gen *MW for (A, B, H)*	Gen *Mvar for (A, B, H)*
1	36.00	0.66
2	72.00	2.61
3	72.00	3.25

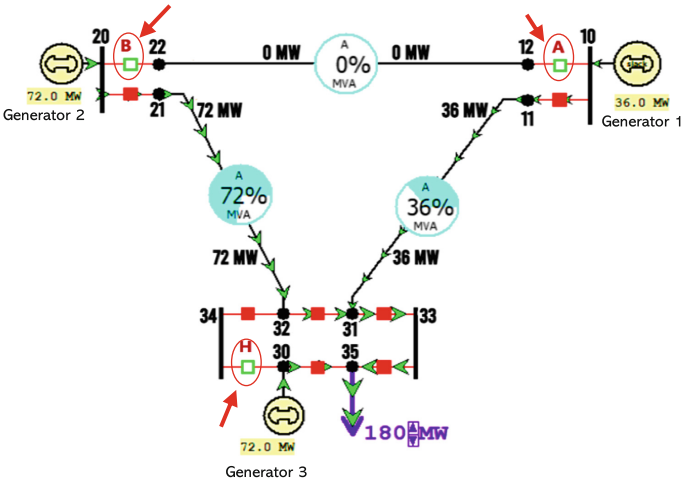


Fig. 3 Attacker compromises the least critical circuit breakers *(A, B, H)*

5 Conclusion and Future Work

In conclusion, this work has summarised the importance of protecting critical infrastructure with smart grid as a case study. Moreover, it emphasises an approach for determining and evaluating the criticality of assets located in OT at physical level. Furthermore, a simulation approach to evaluate the criticality of the physical smart grid system under attack scenarios is also presented, which reflects the potential impact on the physical system. After determining critical assets, our results show that targeting the most critical assets identified in this work can severely compromise the system, making transmission lines to be overloaded beyond their capacities. while targeting the least critical assets is manageable and transmission lines are within the specified range along with stability of the overall system. In the future, we aim to extend this work to determine critical assets at higher levels with a scalable system (e.g., 37-bus case). Moreover, we aim to build a comprehensive methodology to compute and quantify criticality for assets starting from enterprise until the process level assets associated with processes and operations.

References

1. European Commission: European Technology Platform, *Energy*, vol. 19, no. 3, p. 44 (2006). http://europa.eu.int/comm/research/energy. Accessed 22 Feb 2021
2. Ten, C., Manimaran, G., Liu, C.: Cybersecurity for critical infrastructures: attack and defense modeling. IEEE Trans. Syst. Man Cybern. Part A Syst. Hum. **40**(4), 853–865 (2010)
3. Lee, R.M., Assante, M.J., Conway, T.: Analysis of the cyber attack on the Ukrainian power grid defense use case. In: Electricity Information Sharing and Analysis Center, p. 36 (2016). https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
4. Corallo, A., Lazoi, M., Lezzi, M., Pontrandolfo, P.: Cybersecurity challenges for manufacturing systems 4.0: assessment of the business impact level. IEEE Trans. Eng. Manage. (2021)
5. Frankenfield, J.: Zero-Day Attack Definition, 8 May 2020. https://www.investopedia.com/terms/z/zero-day-attack.asp . Accessed 10 Jul 2021
6. Hasan, K., Shetty, S., Ullah, S., Hassanzadeh, A., Hadar, E.: Towards optimal cyber defense remediation in energy delivery systems. In: IEEE GLOBECOM (2019)
7. Vallant, H., Stojanović, B., Božić, J., Hofer-Schmitz, K.: Threat modelling and beyond-novel approaches to cyber secure the smart energy system. Appl. Sci. **11**(11) (2021)
8. HYTEPS: Reduce your reactive power improves efficiency and saves costs, *HYTEPS* (2019). https://hyteps.com/power-quality/reactive-power/. Accessed 11 Jul 2021
9. Corallo, A., Lazoi, M., Lezzi, M.: Cybersecurity in the context of industry 4.0: a structured classification of critical assets and business impacts. Comput. Ind. **114**, 103165 (2020)
10. Crespo, A., et al.: Criticality analysis for improving maintenance, felling and pruning cycles in power lines. IFAC-PapersOnLine **51**(11), 211–216 (2018)