EAI Endorsed Transactions
on Energy Web

Research Article EAI.EU

Real-Time Co-Simulation for the Analysis of Cyber Attacks Impact on Distance Relay Backup Protection

Nadia Boumkheld[1,*], Geert Deconinck[2] and Rick Loenders[3]

[1]KU Leuven, Belgium, nadia.boumkheld@kuleuven.be
[2]KU Leuven, Belgium, geert.deconinck@kuleuven.be
[3]KU Leuven, Belgium, rick.loenders@kuleuven.be

Abstract

Smart Grid is a cyber-physical system that incorporates Information and Communication Technologies (ICT) into the physical power system, which introduces vulnerabilities to the grid and opens the door to cyber attacks. Wide area protection is one of the most important smart grid applications that aims at protecting the power system against faults and disturbances, which makes it an attractive target to cyber attacks, aiming at compromising the reliability of the power system. Understanding the interaction between the cyber and physical components of the smart grid and analyzing the damage that cyber-attacks can do to wide area protection is very important as it helps in developing effective mitigation approaches. This paper evaluates the impact of cyber attacks on a wide area distance relay backup protection scheme in real-time, through the development of a co-simulation platform based on Real Time Digital Simulator (RTDS) and network simulator 3 (NS3) and using the IEEE-14 bus power system model.

Keywords: Real-time co-simulation, Distance relay backup protection, Cyber-physical systems, Cyber attacks

Received on 28 October 2023, accepted on 07 January 2024, published on 16 January 2024

doi: 10.4108/ew.4862

1. Introduction and related work

Wide area protection (WAP) in smart grid refers to the use of smart components and technologies (sensors, protocols...) to collect useful information at different grid locations and perform rapid decisions, to prevent wide-area disturbances/faults and maintain the normal operation of the power system. The use of information and communication technologies (ICT) in wide area protection offers a better protection and improves the reliability of the power system, by providing a real-time communication of information and coordination between system components. Furthermore, it allows the development of many intelligent wide-area schemes such as [1]:

- Remedial Action Scheme (RAS): used to detect predetermined system conditions and take fast corrective Actions such as tripping generation, load shedding, line tripping. . .
- Wide area backup protection relies on the communication between relays and control centers to ensure a fast clearance of faults.
- Emergency protection: wide-area infrastructure allows the prediction of power disturbances and the performance of emergency actions, to prevent unfortunate events such as cascading outages.

Nevertheless, these communication technologies introduce vulnerabilities that serve as entry points for cyber attacks, which compromise the confidentiality, availability and integrity of the data exchanged between the different components of the system. Among these attacks: False data injection (FDI) which consists of modifying data such as control commands or breaker statuses with an aim to

[*]Corresponding author. Email: nadb1899@gmail.com

destabilize the system and prevent protection applications from making the right decisions. Denial of service (DOS) attacks which aim at flooding the network resources leading to data transmission delays and unavailability of protection components. Eavesdropping or sniffing the traffic data allows the attacker to gather significant information such as bus voltages, active power, among others, that can be used to identify vulnerable system components and attack them. An attacker can also place himself/herself in the middle of a communication to intercept the data transmitted between a source and destination and perform malicious actions on it, such as dropping, delaying... this is called a Man In the Middle (MITM) attack. Coordinated attacks are generated by combining multiple attack vectors and can have severe impacts such as cascading outages.

To better understand the effects of cyber attacks on wide area protection, it is important to consider the cyber-physical nature of the smart grid, which combines the power system and the communication network. To serve this purpose both systems need to be simulated to capture their interactions and develop realistic wide area protection scenarios with cyber attacks. This integration of two simulation environments is known as co-simulation, which provides a platform to study and analyze the impact of cyber attacks on wide area protection and allows the development of adequate cyber defense mechanisms in the future. Co-simulation has been used in many smart grid applications, for example in demand response (DR) and dynamic pricing (DP) [2] evaluated the performance of power scheduling algorithms on smart grid household appliances in real time, by developing a co-simulator based on Gridlab-D for the power distribution system simulation and CORE for the communication network. In [3] authors considered two applications: demand/response and market/dynamic pricing and evaluated their performance under different conditions: i. normal operation, ii. network attacks that consist of false data injection and DOS, and iii. network's quality of service. To achieve that they used an existing co-simulation platform: Fenix framework for Network Co-Simulation (FNCS) which is built with Gridlab-D, MATPOWER, and Network Simulator 3 (NS3). Gridattacksim [4] is a co-simulation framework based on GridLAB-D for power system simulation, NS3 for the communication network simulation and the framework for network co-simulation (FNCS). It evaluated the impact of security threats, namely false data injection and jamming attacks on smart grid demand/response and dynamic pricing applications. In wide area monitoring (WAM), [5] is a real time co-simulation platform that studied the impact of ICT systems on wide area monitoring and control applications. It was developed using Simulink and OPAL-RT for the power system simulation, OPNET as a communication system simulator, and SoftPMU that runs in OPAL-RT and collects real time phasor measurements to send them to the communication network. The case study tested with this platform considered five phasor measurement units (PMUs) collecting real-time voltage phasors and sending the data streams to mode estimation and average frequency monitoring applications through a communication network. [6] is a co-simulation framework developed for wide area monitoring which integrates OpenDSS for power system simulation and OMNET++ for communication network simulation. It studied different applications such as a hybrid state estimation algorithm, and renewable energy sources integration in smart grid. In wide area protection, which is the focus of this work, [7] studied the impact of malware-based coordinated attacks on the remedial action scheme (RAS) used to secure power systems in case of disturbances. The attack consists of installing malware on the RAS controller (that controls the power generation by reducing it in case of faults, or keeping the normal generation when the faults are cleared) to turn it to an attacker's bot, and then performing a malicious tripping of a line connected to the generator to create an overload, followed by a pulse attack on the generator which consists of changing the generation by increasing it and decreasing it continuously. The attack was implemented on the PowerCyber cyber physical system (CPS) security testbed, developed by Iowa State University. Global Event-Driven Co-Simulation framework GECO [8] is a co-simulation platform developed with Network Simulator 2 (NS2) and Positive Sequence Load Flow (PSLF) power system simulator. It studied a backup distance relay protection application that involves the communication between the backup distance relay agents and a master agent for supervisory protection, and the peer-to-peer communication between relay agents for the ad-hoc protection. This paper aims at studying and demonstrating the real time impact of cyber attacks on a wide area backup protection application. This application relies on the communication between backup distance relays (slaves) and the Supervisory Control and Data Acquisition (SCADA) control center (master), to make a decision about tripping circuit breakers after the occurrence of a fault. This allows a faster tripping for backup protection and adds robustness and reliability to the protection system, by avoiding false tripping due to relays' errors. To achieve our purpose, we develop a real-time co-simulation platform based on Real Time Digital Simulator (RTDS) and NS3 network simulator. The wide area protection case study in this work is based on the supervisory communication-based distance relay backup protection scheme studied in [8], with added modifications such as considering four distance relay protection zones instead of three and a simple decision-making algorithm for the backup protection. Table 1 summarizes all the mentioned co-simulation platforms. To the best of our knowledge, there has not been any co-simulation platform for studying real-time cyber physical effects of cyber attacks on wide area backup protection.

The remainder of this paper is organized as follows: Section II describes the wide area backup protection application; section III gives a detailed description of the co-simulation platform. The simulation results illustrating the impact of the cyber attacks on the power system are presented in section IV. Finally, the paper is concluded in section V.

Table 1. The co-simulation platforms

Platform	Existing or new	Case study	Power simulator	Network simulator	Type	Cyber Attacks
[2]	New	Evaluation of power scheduling algorithms on household appliances	Gridlab-D	CORE	Real-time	NA
[3]	Existing: FNCS	Evaluation of DR and DP performance with cyber attacks and different network conditions	Gridlab-D	NS3	offline	DOS & data injection
Gridattacksim	New	Impact of FDI and jamming attacks on DR and DP applications	Gridlab-D	NS3	offline	FDI & jamming
[5]	New	Impact of ICT systems on wide area monitoring and control applications	Simulink & OPAL-RT	OPNET	Real-time	NA
[6]	New	Study of WAM applications such as state estimation in smart grid	OpenDSS	OMNET++	offline	NA
[7]	Existing: PowerCyber	Impact of malware based coordinated attacks on the RAS for wide area protection	RTDS/ Opal-RT	Protocols...	Real-time	Coordinated attacks
GECO	New	Study of wide area backup protection in centralized and ad-hoc modes	PSLF	NS2	offline	NA
This co-simulation platform	New	Effects of cyber attacks on distance relay backup protection	RTDS	NS3	Real-time	DOS & ARP Spoofing

2. The Communication Distance Relay Backup Protection Scheme

Distance relays are commonly used for transmission line protection. They measure the impedance from their installation point to the fault location, and they react when the ratio of voltage and current is within a predetermined value range, described as impedance zones. In this paper, four typical impedance zones are selected for the case study as shown in Figure 1.

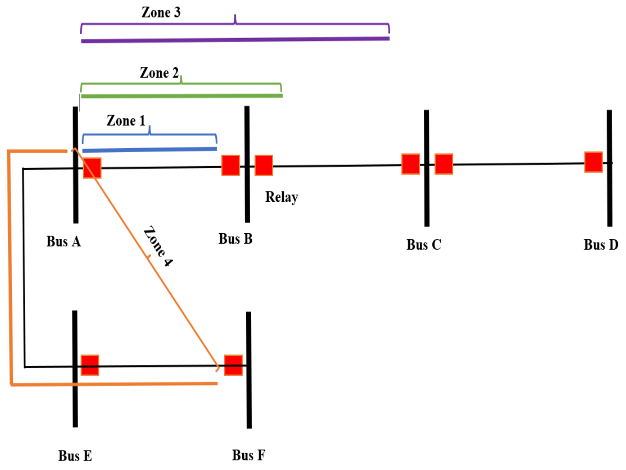
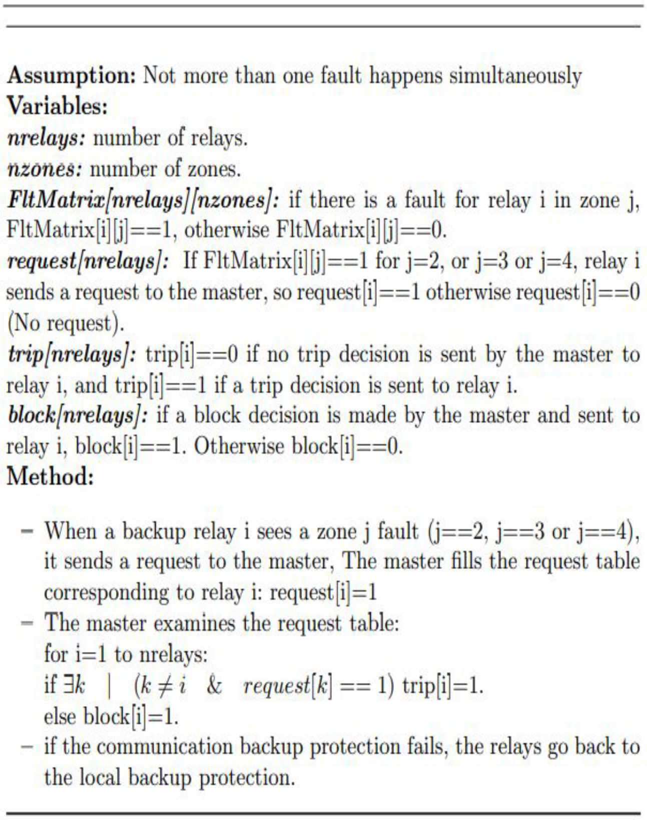


Figure 1. Distance relay protection zones

The first zone (z1) is the primary protection zone, and it covers about 80% of the line length. This zone is set to operate immediately. The second zone (z2) offers protection beyond the intended transmission line, commonly covering 120% of the line impedance, and is set with an operate delay of 200 ms. Based on sensitivity studies, many possible setting combinations exist for the remaining zones. However, for simplification, both zone 3 (z3) and zone 4 (z4) will cover 180% of the line impedance, with an operating delay of 950 ms. The first three zones are directed forward towards the transmission line, while the last zone (z4) is reversed, directed backwards. Given that from the second zone the measured impedance reaches beyond the primary transmission line, these zones are considered part of the local backup protection.

Distance relays can experience software or hardware errors that may cause unintended operation(s), such as a false tripping, which can lead to the instability of the power system and sometimes even blackouts. To avoid unstable grid behavior, communication schemes can be used to support the protection operation and increase its reliability, as suggested in [8]. In this approach, communication is established between the distance relays and the SCADA control center (master), which allows the verification of the fault occurrence by the master and therefore avoids false tripping. It also enables a faster tripping compared to the local backup protection. Each distance relay (slave) is equipped with a communication unit that allows it to send and receive signals to and from the master. The relays are connected to the master through a communication network. When a fault happens in one of the lines, the primary protection operation is the same as the local distance protection i.e. the primary relays trip immediately. However, the backup protection operates in a different way: after detecting a zone 2, 3 or 4 fault, the backup relay communicates with the master by sending a request to know if it should trip or not. The master then makes a decision based on the requests received by other backup relays. If at least one of these backup relays sees the fault, the master concludes that there is a real fault happening and sends a trip decision to the relay that made the request. Otherwise, the master decides that there is no fault and sends a block decision (to block the tripping). Should the communication fail (due to network congestion, cyber attacks...) resulting in a delayed tripping (that exceeds the local backup protection tripping delay) or unsuccessful tripping. The relays go back to the local behavior respecting the original backup protection scheme. Figure 2 explains the method used for the decision making of the communication distance relay backup protection scheme.



Assumption: Not more than one fault happens simultaneously
Variables:
nrelays: number of relays.
nzones: number of zones.
FltMatrix[nrelays][nzones]: if there is a fault for relay i in zone j, FltMatrix[i][j]==1, otherwise FltMatrix[i][j]==0.
request[nrelays]: If FltMatrix[i][j]==1 for j=2, or j=3 or j=4, relay i sends a request to the master, so request[i]==1 otherwise request[i]==0 (No request).
trip[nrelays]: trip[i]==0 if no trip decision is sent by the master to relay i, and trip[i]==1 if a trip decision is sent to relay i.
block[nrelays]: if a block decision is made by the master and sent to relay i, block[i]==1. Otherwise block[i]==0.
Method:

- When a backup relay i sees a zone j fault (j==2, j==3 or j==4), it sends a request to the master, The master fills the request table corresponding to relay i: request[i]=1
- The master examines the request table:

```
for i=1 to nrelays:
if $\exists k \;\mid\; (k \neq i \;\;\&\;\; request[k] == 1)$ trip[i]=1.
else block[i]=1.
```

- if the communication backup protection fails, the relays go back to the local backup protection.

Figure 2. The decision-making algorithm of the communication distance relay backup protection scheme

3. The Co-Simulation Platform

3.1. The Power System Simulation

1. The simulation platform: The simulation of the power system is in real-time and is done with the RTDS simulator, which consists of hardware and software to perform real-time Electro-Magnetic Transient (EMT) simulation. RTDS can simulate complex networks commonly with a time step of 25-50 µs [9]. RTDS has a component called GTNET card (The RTDS simulator's network interface card) which provides a real-time communication to and from the RTDS simulator via ethernet.

2. The power system simulation: The power system is implemented using a modified IEEE 14 bus system. It has 14 buses, 5 generators, 11 loads and 20 transmission lines. Here we consider six distance relays placed at lines 8, 9 and 13, which correspond to lines 12, 13 and 19 in the original IEEE 14 bus system [10]. Each one of these relays has an interface with the GTNET card of RTDS simulator. Figure 3 illustrates the power system architecture.

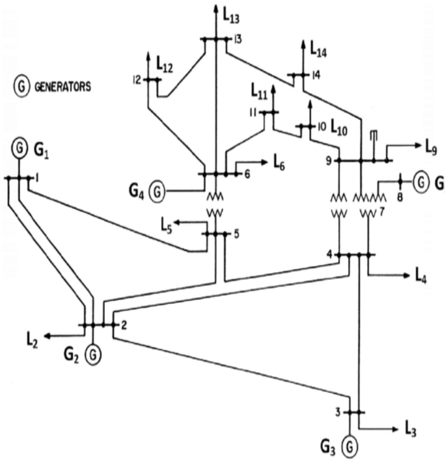


Figure 3. The power system architecture [10]

3.2. The Communication Network Simulation

1. The network simulation platform: to simulate the communication network, we use NS3. It's a discrete-event simulator written in C++ and is an open-source software. NS3 models internet networks and protocols, but also non-internet-based systems can be modelled with NS3. It's a modular simulator as it combines a set of libraries and uses external animators and data analysis tools [11].

2. The network simulation and cyber attacks: to simulate the communication network, an input node with emulated device is used to receive the real data traffic from RTDS using User Datagram Protocol (UDP) sockets and send it through the simulated network. Each distance relay is represented with a node in the NS3 simulation environment. Nodes (relays) that belong to the same substation are in the same Local Area Network (LAN). The master is also a node that is in a different LAN and has an emulated device to be able to send the data to RTDS. Each one of the relay nodes can communicate with the master node through gateways (Routers). Carrier Sense Multiple Access (CSMA) is used to link the nodes located in the same LAN and Point to Point (P2P) links are used between the router nodes. UDP is the transport layer protocol chosen for the communication, because of its connectionless nature, which makes it faster than the Transmission Control Protocol (TCP) and suitable for the protection application. The communication network is IP-based, and the routes are added manually using static routing. The different network parameters are represented in Table 2. The communication network is simulated with two of the most common cyber attacks:

– The DOS attack: The attacker node floods one of the router nodes with UDP traffic, which leads to network congestion and delays the communication between the slave and the master. And when the UDP data rate is too high the packets are dropped and cannot reach their destination, resulting in a failure of the communication between the slave and the master.

– MITM attack (ARP spoofing): The attacker places himself between two hosts A and B. When A wants to connect with B, it broadcasts an ARP request to look for the Media Access Control (MAC) address that corresponds to B's IP address. The attacker sends a fake ARP reply to link his Mac address to B's IP address. He also does the same with A's IP address, this way his MAC address becomes linked to A and B, so he starts receiving all traffic between A and B. By intercepting the traffic between the two hosts, the attacker can perform different malicious actions, such as delaying, dropping, or modifying the data packets before sending them to their destination.
Figure 4 illustrates the communication network simulated with NS3.

Table 2. The network simulation parameters

Parameter	Value
Number of nodes	13
Data link layer protocol	P2P and CSMA
Data rate	100 Mbps
Packets data size	16 bytes for the slave and 8 bytes for the Master
Delay	641 nanoseconds
Transport layer protocol	UDP
Routing form	static

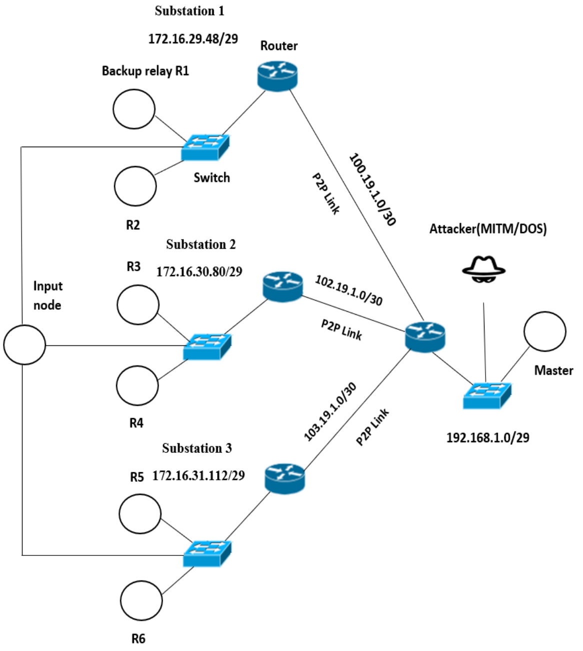


Figure 4. The communication network

3.3. Co-Simulation architecture of the cyber-physical system

The connection between RTDS and NS3 that runs on a Linux machine (with two network interface cards) is achieved through the GTNETx2 card of the RTDS simulator. Each GTNETx2 card has two modules, and each module has one ethernet port. To establish the co-simulation setup for the communication distance relay backup protection application, each module (A and B) of the GTNET component is connected to a physical interface of the Linux machine. The slaves (distance relays) have interfaces with the GTNET module A, and the master has an interface with the GTNET module B. This way the data is calculated at the RTDS simulator, then the GTNET interface corresponding to the distance backup relay (slave) sends the data to the input node in NS3. The latter sends the data to the corresponding relay simulated node; the data is then routed until it reaches the master node, which finally sends it to the master interfaced with the GTNET module B. The data also goes in the other way, from the master to the distance relays. The overall co-simulation model of the communication distance relay backup protection scheme is shown in Figure 5.

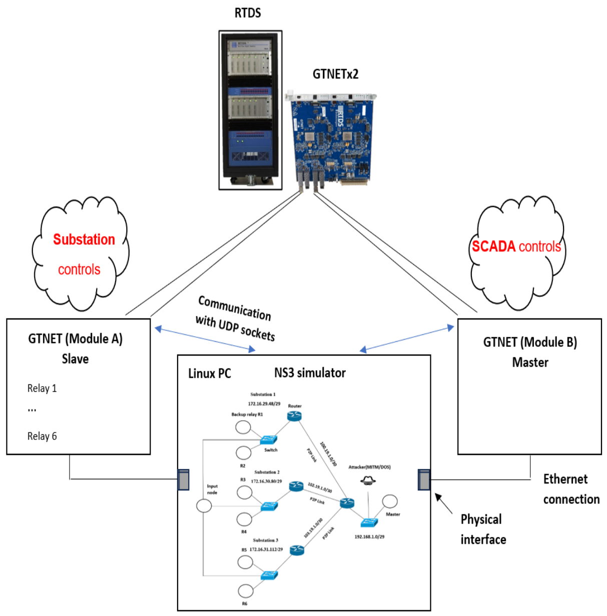


Figure 5. The co-simulation model of the communication distance relay backup protection scheme

4. The Co-Simulation Results

1. with a real fault: to conduct the simulations, a three phase short-circuit fault is generated at 50% of line 13 (between Bus 12 and Bus 13). And both primary relays are dysfunctional (unable to trip and clear the fault), so the backup relays take over. To visualize the attacks' impact on the SCADA communication distance relay backup protection system, we measure the voltage magnitude and current at Bus 14 and at the breakers of the primary protection relays of line 13 respectively, considering three different scenarios:

- Without any Cyber Attack: Figure 6 shows that the voltage magnitude at Bus 14 is initially at 1 (steady state), and when the fault happens the voltage drops. The backup relays send the requests to the master which decides that the fault is real in this case (because it receives the request from more than one backup relay), and then sends the trip response back to the associated backup relays. After the fault is cleared which takes 186 ms, the system voltage (at Bus 14 and beyond) goes back to its normal value. The time to clear the fault using the communication distance relay backup protection is very fast compared to the local backup protection, which would take at least 950 ms in this case. The current's value in Figure 7 also jumps from hundreds to thousands of amperes when the fault happens, and then returns to normal when the fault is cleared.

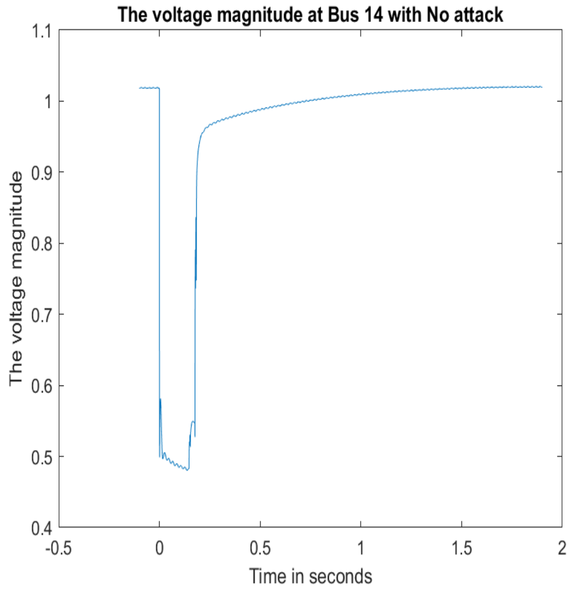


Figure 6. The voltage Magnitude at Bus 14 with No Attack

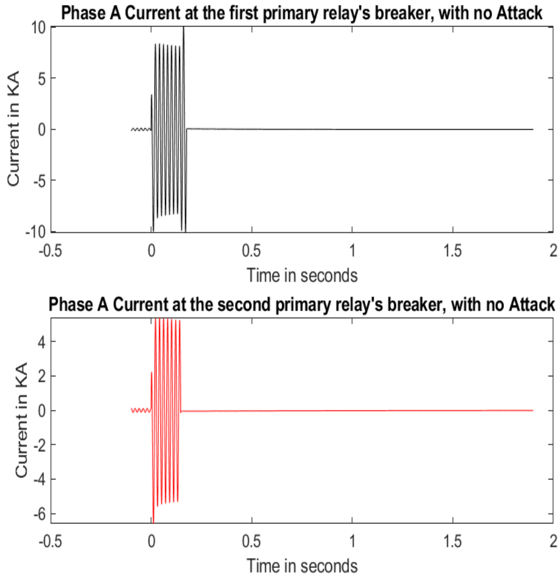


Figure 7. Phase A current at the primary relays' breakers of Line 13 with no attack

- With the MITM attack (ARP spoofing): In this case, the attacker receives a trip command sent by the master to the backup relays and changes it to no trip, so no communication tripping will be done by the backup relays. Figure 8 shows that the voltage value drops at the moment of the fault, and it goes back to the steady state after 1.05 s, because the communication tripping doesn't happen and the control goes back to the local backup protection, consequently the fault takes a longer time to be cleared compared to the case when there is no attack (186 ms). The current value in Figure 9 also goes back to normal when the fault is cleared.

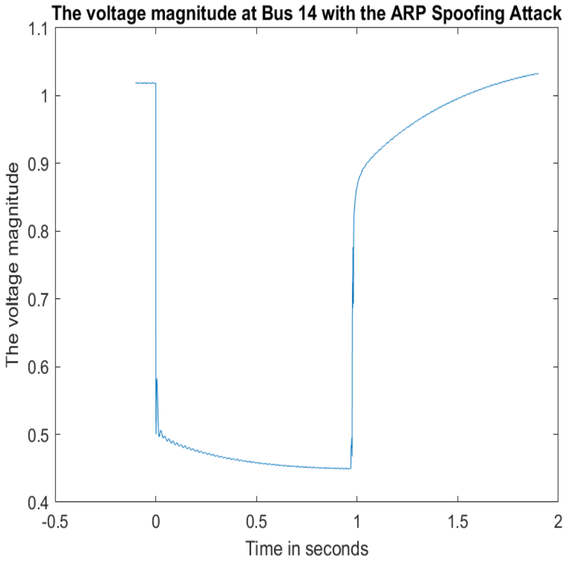


Figure 8. The voltage magnitude at Bus 14 with the MITM attack (ARP spoofing)

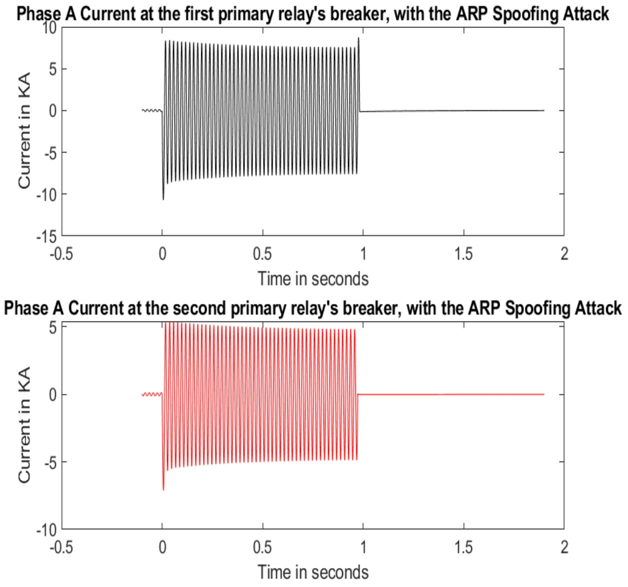


Figure 9. Phase A current at the primary relays' breakers of Line 13 with the MITM attack (ARP spoofing)

- with the DOS attack: The DOS attack is generated by sending UDP traffic with a rate of 15Mbps from an attacker node towards the router located in the master's LAN (the attacker is also in the master's LAN). Figure 10 shows that the fault is cleared, and the voltage goes back to normal after 743ms, which is longer than the time it takes in the absence of cyber attacks (186 ms). The reason for that is that the congestion in the communication network caused by the DOS attack leads to a delay in delivering the trip signals from the master to the distance backup protection relays. Figure 11 shows that the current value also goes back to normal after the fault is cleared.

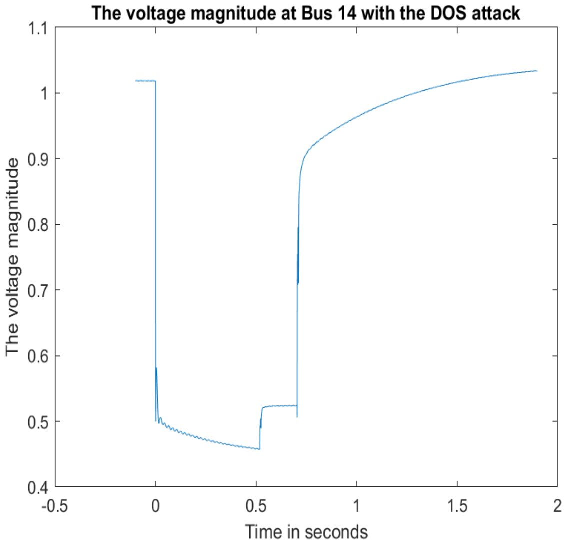


Figure 10. The voltage magnitude at Bus 14 with the DOS attack

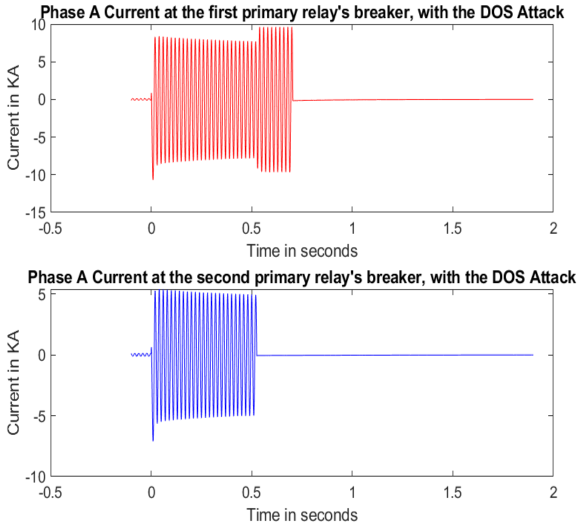


Figure 11. Phase A current at the primary relays' breakers of Line 13 with the DOS attack

2. with a fake fault:

- Without any cyber attack: In this case, there is no fault, but one of the backup relays sends an erroneous fault zone 4 signal to the master. Figure 12 shows that the value of the voltage is not affected, and it stays at 1. The current value also remains normal. This is because the master in this case only receives a request from the relay that detects/fakes the fault and since no other relay sees the fault, the master decides that there is no fault and sends a block signal back to the backup relay, therefore no tripping takes place.

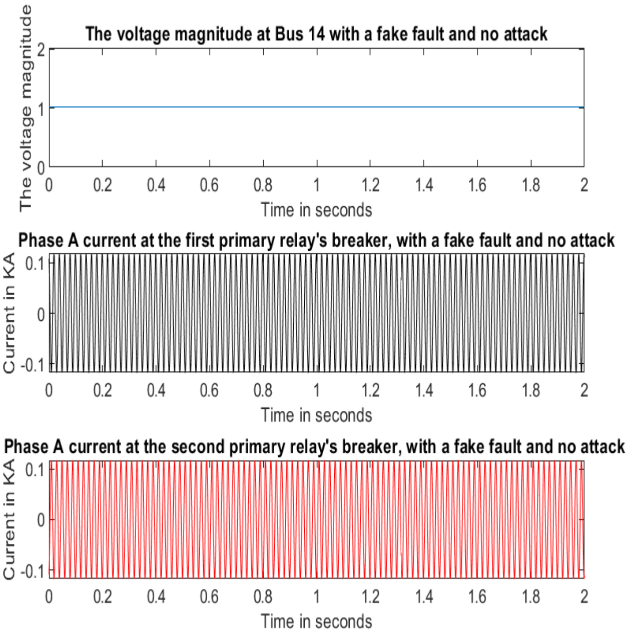


Figure 12. Voltage magnitude at Bus 14 and phase A current at the primary relays' breakers of Line 13 with a fake fault and no attack

- With the MITM attack (ARP spoofing): similarly, to the case without attacks, the backup relay generates the erroneous zone 4 fault, however here the attacker will change the master's decision from block to no block leading to the tripping of the local backup protection. This is shown in Figure 13 where the voltage drops by 0.006 when the trip happens, and the current's value goes from 100 A to 270 A.

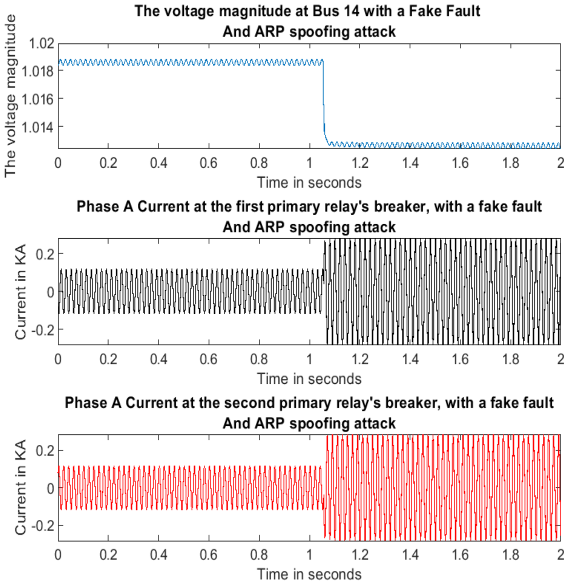


Figure 13. Voltage magnitude at Bus 14 and phase A current at the primary relays' breakers of Line 13 with a fake fault and MITM attack (ARP spoofing)

The results show that the communication distance relay backup protection application can achieve a fast tripping when faults happen, and that it is resilient to fake faults. However, it is also vulnerable to the MITM and DOS attacks which affect the time needed to clear the faults (it becomes longer compared to the case with no attacks), and the resilience against false tripping. This is translated through the values of voltage and current.

5. Conclusion

In this paper, we studied the real-time effects of cyber attacks on wide area backup protection, by considering an application that relies on the communication between backup distance relays and the SCADA control center and developing a co-simulation platform based on RTDS and NS3. Through the experiments, we showed the efficiency of the communication backup protection scheme in terms of faster tripping compared to local backup protection, and its ability to avoid false tripping. We also demonstrated through the experiments how cyber attacks can affect the protection scheme and render it less efficient. In the future work, we will generate a wide range of cyber attacks, and integrate hardware to the co-simulation testbed. Additionally, we will focus on securing the power grid against attacks by developing a robust intrusion prevention system.

Acknowledgements.
This work is a part of the Cyber-Physical Risk of the bulk Electric Energy Supply System (CYPRESS) project. We would like to thank anyone who provided their feedback within the project, and a special thanks and gratitude to Dr. Chamara Devanarayana (Simulation Specialist at RTDS Technologies) who provided tremendous help and documentation about the co-simulation with RTDS and NS3 [12]. We also thank the RTDS support team for their quick responses and assistance with any questions related to RTDS.

References

[1] S. Vahidi, M. Ghafouri, M. Au, M. Kassouf, A. Mohammadi and M. Debbabi. Security of Wide-Area Monitoring, Protection, and Control (WAMPAC) Systems of the Smart Grid. A Survey on Challenges and Opportunities. In IEEE Communications Surveys & Tutorials. 2023; vol. 25 no. 2: pp. 1294-1335.

[2] X. Li, Q. Huang and D. Wu. Distributed Large-Scale Co-Simulation for IoT-Aided Smart Grid Control. In IEEE Access. 2017; vol. 5: pp. 19951-19960.

[3] P. Moulema, W. Yu, D. Griffith, and N. Golmie. On Effectiveness of Smart Grid Applications using Co-simulation. In Proceedings of the 24th International Conference on Computer Communications and Networks (ICCCN) 2015; NIST, Las Vegas.

[4] L. Duy, A. Anwar, S. Loke, R. Beuran, and Y. Tan. GridAttackSim: A Cyber Attack Simulation Framework for Smart Grids. In: Electronics. 2020; 9: no. 8.

[5] D. Babazadeh, M. Chenine, K. Zhu, L. Nordstr¨om, and A. Al-Hammouri. A Platform for Wide Area Monitoring and Control System ICT Analysis and Development. In: Grenoble Conference PowerTech; 2013; Grenoble.

[6] D. Bhor, K. Angappan, and K. Sivalingam. Network and power-grid co-simulation framework for smart grid wide-area monitoring networks. In: Journal of Network and Computer Applications. 2016; vol. 59: pp. 274–284. ELSEVIER.

[7] V. Kumar Singh, A. Ozen and M. Govindarasu. Stealthy cyber attacks and impact analysis on wide-area protection of smart grid. In: North American Power Symposium (NAPS); 2016; Denver, CO, USA. IEEE; pages 1–6

[8] H. Lin, S. S. Veda, S. S. Shukla, L. Mili and J. Thorp: GECO: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network. In: IEEE Transactions on Smart Grid. 2012; vol. 3: pp. 1444-1456.

[9] Rtds-simulator-overview. https://knowledge.rtds.com/hc/en-us/articles/ 8501418280855-RTDS-Simulator-Overview

[10] P. Dey, A. Bhattacharya, and P. Das. Tuning of power system stabilizer for small signal stability improvement of interconnected power system. In: Applied Computing and Informatics IEEE. 2017; Vol. 16 No. 1/2: pp. 3-28.

[11] Ns-3 tutorial. https://www.nsnam.org/docs/tutorial/html/

[12] https://github.com/chamara84/ns3_cybersec

.