Towards Federated Learning-based Collaborative Adaptive Cybersecurity for Multi-microgrids

Svetlana Boudko[1], Habtamu Abie[1][a], Ethiopia Nigussie[2] and Reijo Savola[3]

[1]*ICT Research, Norwegian Computing Center, P.O. Box 114 Blindern, Oslo, Norway*

[2]*Department of Future Technologies, University of Turku, Turku, Finland*

[3]*Security Assurance, VTT Technical Research Centre of Finland Ltd., Oulu, Finland*

Keywords: Multi-microgrid, Machine Learning, Federated Learning, Cybersecurity, Collaborative Protocols, Adaptive Mechanisms.

Abstract: Multi-microgrids (MMGs) provide economic and environmental benefits to society by improving operational flexibility, stability and reliability of a smart grid. MMGs have greater complexity than conventional power networks due to the use of multiple infrastructures, communication protocols, controllers, and intelligent electronic devices. The distributed and heterogeneous connectivity technologies of the MMGs and their need to exchange information with external sources as well as the vulnerabilities in the communication networks and software-based components, make MMGs susceptible to cyberattacks. In this work, we present a conceptual framework for collaborative adaptive cybersecurity that is able to proactively detect security incidents. The framework utilizes federated learning for collaborative training of shared prediction models in a decentralized manner. The methodology used in this research is mainly analytical. This involves analysis of how the principles of a collaborative adaptive cybersecurity can be applied to the MMG environments resulting in the development of theoretical models which can then be validated in practice by prototyping and using real time simulation.

1 INTRODUCTION

Novel and effective solutions for cybersecurity and cyber resilience of multi-microgrids (MMGs) are crucial for their reliable and safe operation. MMG is a cluster of interconnected microgrids (MGs) that are coupled to the main power grid via switch for the purpose of achieving power resilience and stability through fast power exchange. It also enables a smooth and high penetration of distributed energy resources (DERs) in the grid (Wu et al., 2018; Goyal and Ghosh, 2016) and provides operational, economic, environmental and sustainability benefits to society (Anastasiadis et al., 2010; Saad et al., 2011). As shown in Fig. 1, the MMG's physical system is composed of multiple two-way interconnected systems such as DER, energy storage systems (ESS), active loads (e.g. electric vehicles,), fixed loads and controllers. Its cyber system has greater complexity due to the use of multiple infrastructures, communication protocols, controllers, intelligent electronic devices (IEDs), smart meters and phasor measurement units. The distributed and heterogeneous connectivity technologies of the MMGs and their need to exchange information with external sources as well as the vulnerabilities in the communication networks and software-based components, make MMGs susceptible to cyberattacks. High profile cyberattacks on power systems had been launched by various actors. The cyberattacks that impaired the Ukrainian power system in 2015 and 2016, which left 250,000 people without power for several hours, were due to the vulnerability of the substation communication protocol to false data injection attack (FDIA) (Whitehead et al., 2017). Suspicious cyber events within the power grid of US were reported in 2020 (OE-, 2020). Cyber incidents in MMGs include various attacks, such as bias injection, zero dynamics, denial of service, eavesdropping, replay, stealthy, covert, dynamic false data injection and time synchronization attacks (Pasqualetti et al., 2013). Stealthy attacks can easily penetrate the networked systems without altering the system observability (Zhao et al., 2018).

Since attacks targeting critical infrastructures are becoming stealthy, complex and continuously evolv-

[a] https://orcid.org/0000-0003-0866-5050

Boudko, S., Abie, H., Nigussie, E. and Savola, R.
Towards Federated Learning-based Collaborative Adaptive Cybersecurity for Multi-microgrids.
DOI: 10.5220/0010580700830090
In *Proceedings of the 18th International Conference on Wireless Networks and Mobile Systems (WINSYS 2021)*, pages 83-90
ISBN: 978-989-758-529-6

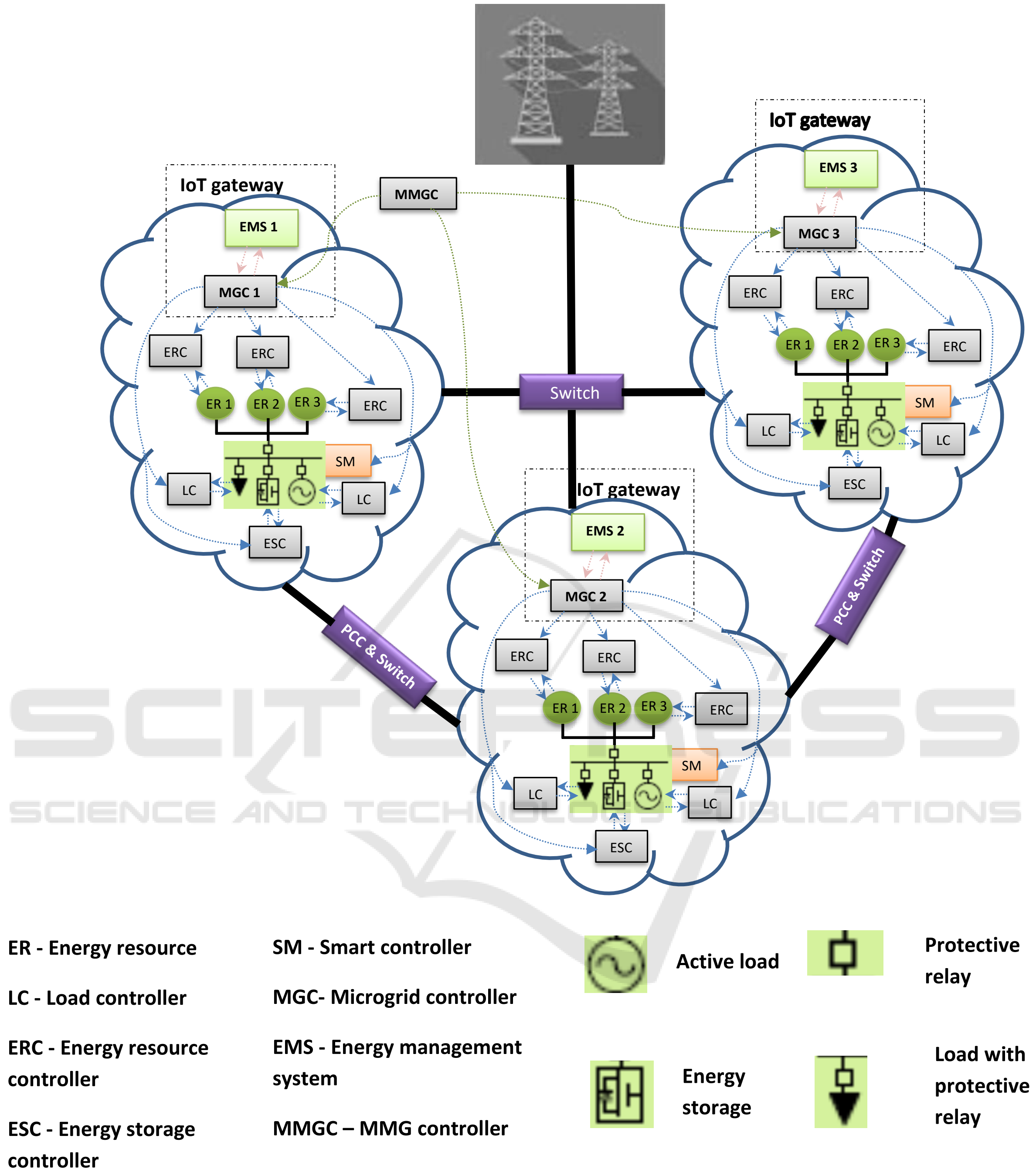

Figure 1: Multi-Microgrid Architecture.

ing, conventional security measures fail to detect and prevent. Therefore, proactive cybersecurity and cyber resilience solutions are required to ensure their safety, security and reliability of MMGs. To be effective, these solutions need to comply with complexity and diversity of critical infrastructures and to adapt to constantly evolving attacks. To address highly-distributed and heterogeneous nature of MMGs, we intend to utilize the federated learning concept to facilitate collaborative and decentralized training of proactive detection models and outline the conceptualization of the overall collaborative adaptive approach. For this purpose, we analyse the measures needed to improve security protection of MMGs, and propose the collaborative adaptive security implementation roadmap.

The work proposed in this paper includes the following contributions: 1) analysis of federated learning, intrusion detection, adaptivity, multi-layer feedback loops, and collaboration; 2) conceptualisation and analysis of a framework for federated learning-based collaborative adaptive cybersecurity; and 3) roadmap for implementation.

2 RELATED WORK

Researchers have proposed intrusion detection systems (IDSs) for MG as one of the defence mechanisms (Ameli et al., 2020; Lu et al., 2019; Zhang et al., 2019; Habibi et al., 2020; Vu et al., 2019). These IDSs focus on detection of specific attack(s), and/or malicious activities in subsystem(s)/process(es) in MGs. FDIA detection has got much attention as it can impede several MG functionalities, such as frequency/voltage restoration (Lu et al., 2019; Abhinav et al., 2018a; Abhinav et al., 2018b), load sharing (Zhang et al., 2019) and state estimation (Zhao et al., 2018). Furthermore, most of the proposed IDSs target a single MG without considerations of changes in threat landscape when it is interconnected with other MGs (MMG). Conventional host-based or network-based IDSs that operate individually at a single layer are not scalable to large networked systems nor to massively parallel attacks targeting different layers and components, resulting in low detection performance. In MMG, a skilled intruder can slowly change the behaviour to avoid detection by independently operating IDSs.

Recently, efforts have been made in the development of collaborative IDSs in smart grid (Nikmehr, 2019). Collaborative IDSs can analyse evidence from multiple domains simultaneously through distributed monitoring agents to create a holistic view of the activities in MMG. In addition to collaborative, cross-layered operation of IDSs is necessary to detect intrusions at perception, network and application layers of MMG. Adaptability of the detection and prevention mechanisms are also crucial as the threats in critical infrastructures are often dynamically changing to evade detection. To address the anomaly detection problem of cyber-physical systems, the study (Xu et al., 2021) presents a novel digital twin-based solution. The solution consists of a timed automaton-based digital twin model and a GAN-based anomaly detector.

Surveys and taxonomies of adaptive security can be found from (Elkhodary and Whittle, 2007; Yuan and Malek, 2012). The study (Bakhsh et al., 2019) proposes an adaptive IDS to enhance security along with the growth of connected devices. Security metrics provide the on-line means with which to score security countermeasure effectiveness. The metrics approaches that are most valuable for adaptive security focus on cybersecurity objectives. Security objective decomposition–based metrics approaches were proposed in (Savola and Abie, 2009). Summaries of security metrics approaches are reported in (Savola and Abie, 2009; Herrmann, 2007; Jaquith, 2007; Pendleton et al., 2016).

There exist various adaptive architectures and frameworks. These include ACT-R (Adaptive Control of Thought—Rational) (Oltramari et al., 2013) for cognitive-based decision support in cyber operations, OODA (observe, orient, decide, act) cycle for cyber-situational awareness (Lenders et al., 2015), MAPE-K (monitor, analyse, plan, execute, knowledge) cycle for autonomic computing capabilities (self-configuring, self-healing, self-optimizing, and self-protecting) (ibm, 2005), etc. Our model is similar to most of these frameworks in that it models the basic monitor-analyse-adapt cycle in an efficient way but differs in that it combines the decide-act or plan-execute cycles into the adapt phase for optimization purpose for constrained devices and the knowledge is distributed among the three phases unlike the centralized knowledge of the MAPE-K cycle. We believe that the decide-act or plan-execute cycles are natural activities of the adapt single phase.

There have been several studies performed on federated learning (McMahan et al., 2017). It is a relatively new research initiative that utilizes distributed ML approach. In (Brisimi et al., 2018), a decentralized optimization framework was developed that enables multiple data holders to collaborate and converge to a common predictive model in a decentralized manner. Sparse Support Vector Machine (sSVM) classifier was used. The authors developed an iterative cluster Primal Dual Splitting (cPDS) algorithm for solving the large-scale sSVM problem. The authors claim that cPDS converges faster than centralized methods at the cost of some communication between agents.

In (Preuveneers et al., 2018), the authors present a permissioned blockchain-based federated learning method for anomaly detection on the distributed ledger. Federated learning is integrated with blockchain technology without centralizing the training data. The authors achieved full transparency over the distributed training process of the neural network.

In (Nguyen et al., 2019), the authors present an autonomous self-learning distributed system for detecting compromised IoT devices. The solution uses unlabeled data and does not require any human intervention. The authors demonstrated the efficacy of anomaly detection in detecting a large set of malicious behaviour from devices infected by the Mirai malware.

In (Zhao et al., 2019), a multi-task deep neural network in federated learning was proposed to perform network anomaly detection task, VPN traffic recognition task, and traffic classification task, simultaneously. The results showed that the multi-task method reduced training time overhead compared with multiple single-task models.

In (Mothukuri et al., 2021), Long Short Term Memory Networks and Gated Recurrent Units were utilized to build a federated learning-based solution for anomaly detection on the IoT networks. The authors showed that their solution ensured the privacy of user data and outperformed the non-FL version of intrusion detection algorithms.

In our analysis, we recognise that certain research has been done on applying federated learning to detect anomalies and attacks in distributed environments. However, a problem of detecting and predicting security incidents in MMG systems is not thoroughly addressed. The dynamic, distributed and heterogeneous nature of these systems needs to be carefully analysed. Further research on how to integrate federated learning and adaptive security techniques is also required.

3 PROPOSED COLLABORATIVE ADAPTIVE APPROACH

Adaptive security refers to a security solution that learns and adapts to the changing environment during run-time in the face of changing threats and anticipated threats before they are manifested. The response can be by (i) adjusting internal parameters, such as encryption schemes, security protocols, security policies, security countermeasures, or (ii) making dynamic changes in the structure of the security system (Shnitko, 2003; Abie and Balasingham, 2012). This is an approach for a real-time monitor-analyze-adapt optimized cycle for IoT and it will be extended for multi-microgrids without loosing any clarity or functionality.

3.1 Adaptation Loop with Federated Learning Component

As seen in Fig. 2, the system employs various components. It will be developed using collaborative distributed adaptive monitoring and control agents, hybrid security incident detection technique (signature, specification, anomaly), data-driven situational awareness, collaborative and cross-layered protocols as well as adaptability methods.

Adaptive Monitoring is necessary for adjusting threat detection thresholds dynamically according to the local and global context of the environment. **Adaptive Monitoring** continuously collects, aggregates, filters and reports contextual information received from both internal and external MMG environments using sensors.

Adaptive Security Management employs adaptivity mechanisms, decision making, and metrics-based security enforcing actuators. It comprises of **Analytics Module** and **Adaptive Models**. **Analytics Module** processes this information using the federated learning models and context and location awareness. The results of this analysis are used to dynamically estimate and predict security and privacy incidents. **Adaptive Models** use security actuators and countermeasures to adapt to the dynamism of MMGs, their interactions, and the environments, and to the varying degrees of security incidents that the MMG system will be compromised. These models can utilize security measurement and metrics for quantitative measures by which MMG security solutions can be evaluated.

MMG uses heterogeneous networks and devices as well as diverse processes. To address distributed dynamic and heterogeneous features of MMG, we consider federated learning approach where training of a ML model is coordinated between multiple agents. The model training is done in a decentralized manner on various edge devices using their local data and thus the local data are not shared with any other participating devices. A random subset of agents is selected for training for each training round. Their local data and computational resources are used to compute the new weights of the model. It serves as the main component of **Analytics Module**.

This solution improves scalability, allows for lower latency and less power consumption, and helps to preserve privacy. To better control privacy exposure, federated learning can be reinforced by privacy preserving methods such as differential privacy (Dwork, 2006) and secure multiparty computation (Frikken, 2011). The other advantage of using federated learning is the ability to deal with unbalanced, sparse and non-representative data at local nodes. This fits well into distributed nature of MMGs. A global ML model will be created from local ML models trained by multiple MGs. This will make the MGs better adapted to their local threats and will provide mechanisms for sharing the knowledge about new

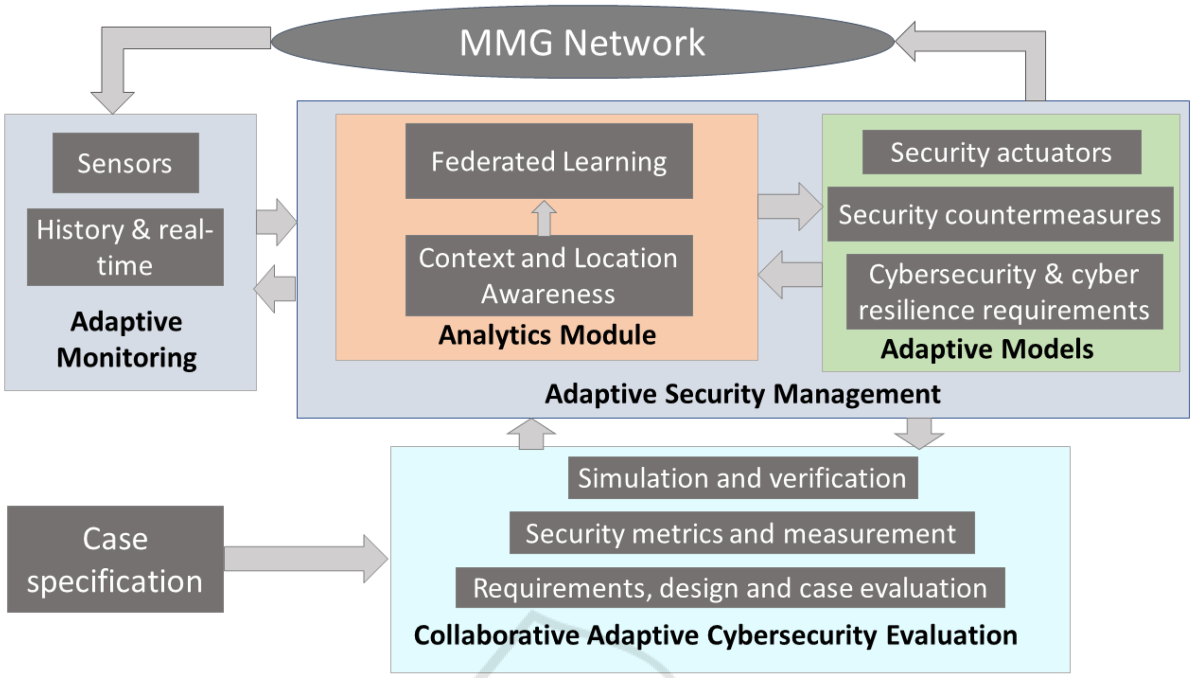
MMG Network
Sensors
History & real-time
Adaptive Monitoring
Federated Learning
Context and Location Awareness
Analytics Module
Security actuators
Security countermeasures
Cybersecurity & cyber resilience requirements
Adaptive Models
Adaptive Security Management
Simulation and verification
Security metrics and measurement
Requirements, design and case evaluation
Collaborative Adaptive Cybersecurity Evaluation
Case specification

Figure 2: Adaptation loop for adaptive monitoring, analytics and federated learning, and adaptive models.

types of attacks among the community of the MGs. Poisoned attacks also need to be carefully studied.

The evaluation of the developed cybersecurity system is done by **Collaborative Adaptive Cybersecurity Evaluation**. It concretizes the results of the analysis and adaptivity by demonstrating the validity of the system through well-designed case study, security metrics and verification method.

3.2 Main Components of Collaborative Adaptive Approach

Fig. 3 depicts the main components of the proposed collaborative adaptive approach. Each component implements the adaptation (monitor-analyse-adapt) loop depicted in Fig. 2 and can use evaluation metrics to evaluate the analysis and adaption. The main components are as follows. MGCollAdapter is an MG local collaborative adaptive model with the necessary functionality to monitor, predict and mitigate cyber-attacks at the MG level. MMGCollAdapters are collaborative adaptive models at the MMGs level with functionality monitoring, predicting and mitigating MMGs related attacks. MGCollAdapter, and MMGCollAdapters collaborate with each other to form a global view of the cyberspace with feedback loops using collaboration protocols. ApplCollAdapters are collaborative adapters at the application level for monitoring, predicting and mitigating application related attacks.

These multi-layer feedback loops improve scalability and flexibility for varying devices in increasing complexity. For instance, certain activities occur at very rapid speeds requiring a very tight feedback loop to support adaptive control. Other activities occur on a longer timescale and adaptive control algorithms may need to consider a wider range of factors in a slow feedback loop. The challenge is then the correlation of cause and effect of actions due to the variety of temporal loops and their dramatic speed differences. The specific challenge is to design algorithms that adapt to the constraints and capabilities of the different devices, as well as to the possible dynamicity of these constraints and capabilities. The approach uses federated learning model with a single hidden layer to run it on resource constrained devices, with more hidden layers to run it on edge devices to enhance the capability of learning better features to represent edge data, and with deep hidden layers to run it on more computationally powerful devices to improve the detection and prediction accuracy and to reduce the detection delay. The Adapters act as autonomous systems in their local environment accomplishing their tasks, achieving their goals, and interacting with their surroundings with no human involvement. They can also implement prevention mechanisms autonomously representing the ultimate autonomous level that can be achieved increasing complexity.

Explainable AI Collaborative Adaptive Cyberse-

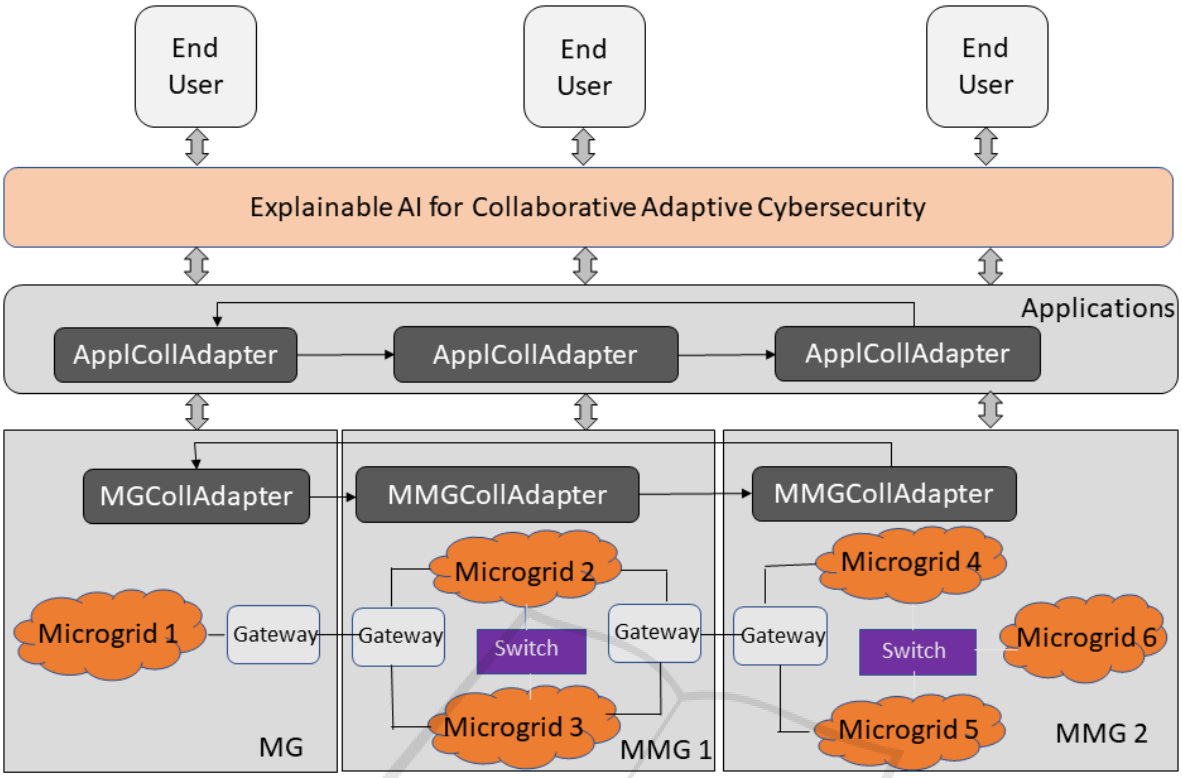

Figure 3: Components of collaborative adaptive cybersecurity of MMGs.

curity implements explainable collaborative adaptive cybersecurity of the MG and MMGs for the stakeholders and end-users. The Explainable AI Models will provide the decision support mechanisms to end-users in their decision making in understandable ways. This will include, among others, monitored information, identification of adaptation options, assessment of the adaptation options, adaptation plans and adaption actions. For this the use of the Shapley-Lorenz decomposition (Giudici and Raffinetti, 2021) that appears as a new explainable artificial intelligence method will be investigated.

Security metrics support development of explainable AI/ML for the purposes of cybersecurity. They enable transparency and traceability of security information, obtained from security functionalities used in training. In AI/ML, transparency consists of traceability, explainability and communication (High-Level Expert Group on AI, 2019).

3.3 Roadmap for Implementation

The components of the proposed approach will be designed, evaluated, and implemented. We consider to address several research challenges. We intend to define architectural design that enables collaborative and cross-layered features of the system, and facilitates functioning of federated learning tasks. In-depth analysis of vulnerabilities and threats in MMGs' network protocols, components and platforms will be carried out. Based on the analysis, we will develop a threat model for identifying a set of potential attacks on MMGs. The capability of various cybersecurity mechanisms in preventing the determined potential attacks will be analysed. The findings of this analysis serve as input to the specification of the system architecture.

Fig. 3 depicts the proposed approach with its various components that implement the adaptation loop for adaptive monitoring, analytics, and predictive models and adaptive models depicted in Fig. 2. Further, we will develop an adaptive detection and prevention of security incidents that is compliant with architecture and requirements of MMG. To proactively detect security incidents, different machine learning and deep learning methods will be evaluated according to the changing and distributed context within the environment. We plan to evaluate convolutional neural networks, recurrent neural networks, deep belief networks, and a set of ensemble methods within the context of distributed learning. Several open datasets exist and can be applied for training and evaluating the models (Ferrag et al., 2020). Based on the evaluation results, the system will select and apply the methods that prove to be most effective in current observations. To evaluate the effectiveness of the component, a set of metrics will be used. We intend to use high accuracy, low false positive rate, trustworthiness, scalability, flexibility. Decision criteria will be defined and applied.

A set of relevant cybersecurity countermeasures for the adaptive security management will be developed, along with their operational adaptivity logic based on security metrics and context and location information. Adaptive security management functionalities will be designed. The goal is an efficient self-protecting monitor-analyze-adapt mechanism, which will rely on learning and adapting to the changing context and location, anticipating threats. The approach will be cross-layered and federated.

4 CONCLUSION AND FUTURE WORK

This paper defines the conceptualization and the roadmap for collaborative adaptive cybersecurity of multi-microgrids. Federated learning is utilized to facilitate collaboration and to support adaptation in a distributed and heterogeneous context. We have studied the literature and outlined system architecture and components required for the development and implementation. At this stage, our work is in the concept phase. We plan to facilitate and evaluate federated learning process, develop adaptive security management, implement prototypes and validate them regarding system complexity, processing time, adaptivity, stability, security requirements. We intend to validate the feasibility of the approach using real time simulation.

ACKNOWLEDGEMENTS

This work has been carried out in the context of the Center for Research-based Innovation NORCICS, funded by the Research Council of Norway, grant number 310105/F40, and the FINSEC project (contract number 786727) funded by the European Commission in the scope of its H2020 program.

REFERENCES

(2005). An architectural blueprint for autonomic computing. Technical report, IBM.

(2020). Oe-417 electric emergency and disturbance report. Technical report.

Abhinav, S., Modares, H., Lewis, F. L., Ferrese, F., and Davoudi, A. (2018a). Synchrony in networked microgrids under attacks. *IEEE Transactions on Smart Grid*, 9(6):6731–6741.

Abhinav, S., Schizas, I. D., Lewis, F. L., and Davoudi, A. (2018b). Distributed noise-resilient networked synchrony of active distribution systems. *IEEE Transactions on Smart Grid*, 9(2):836–846.

Abie, H. and Balasingham, I. (2012). Risk-based adaptive security for smart iot in ehealth. In *Proceedings of the 7th International Conference on Body Area Networks*, BodyNets '12, page 269–275, Brussels, BEL. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Ameli, A., Hooshyar, A., El-Saadany, E. F., and Youssef, A. M. (2020). An intrusion detection method for line current differential relays. *IEEE Transactions on Information Forensics and Security*, 15:329–344.

Anastasiadis, A. G., Tsikalakis, A. G., and Hatziargyriou, N. D. (2010). Operational and environmental benefits due to significant penetration of microgrids and topology sensitivity. In *IEEE PES General Meeting*, pages 1–8.

Bakhsh, S. T., Alghamdi, S., Alsemmeari, R. A., and Hassan, S. R. (2019). An adaptive intrusion detection and prevention system for internet of things. *International Journal of Distributed Sensor Networks*, 15(11):1550147719888109.

Brisimi, T. S., Chen, R., Mela, T., Olshevsky, A., Paschalidis, I. C., and Shi, W. (2018). Federated learning of predictive models from federated electronic health records. *International Journal of Medical Informatics*, 112:59–67.

Dwork, C. (2006). Differential privacy. In *33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006)*, volume 4052 of *Lecture Notes in Computer Science*, pages 1–12. Springer Verlag.

Elkhodary, A. and Whittle, J. (2007). A survey of approaches to adaptive application security. In *Proceedings of the 2007 International Workshop on Software Engineering for Adaptive and Self-Managing Systems*, SEAMS '07, page 16, USA. IEEE Computer Society.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., and Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50:102419.

Frikken, K. B. (2011). *Secure Multiparty Computation (SMC)*, pages 1121–1123. Springer US, Boston, MA.

Giudici, P. and Raffinetti, E. (2021). Shapley-lorenz explainable artificial intelligence. *Expert Systems with Applications*, 167:114104.

Goyal, M. and Ghosh, A. (2016). Microgrids interconnection to support mutually during any contingency. *Sustainable Energy, Grids and Networks*, 6:100–108.

Habibi, M. R., Baghaee, H. R., Dragičević, T., and Blaabjerg, F. (2020). Detection of false data injection cyberattacks in dc microgrids based on recurrent neural networks. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pages 1–1.

Herrmann, D. S. (2007). *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*. Auerbach Publications, USA, 1st edition.

High-Level Expert Group on AI (2019). Ethics guidelines for trustworthy ai. Report, European Commission, Brussels.

Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley Professional.

Lenders, V., Tanner, A., and Blarer, A. (2015). Gaining an edge in cyberspace with advanced situational awareness. *IEEE Security Privacy*, 13(2):65–74.

Lu, L., Liu, H. J., Zhu, H., and Chu, C. (2019). Intrusion detection in distributed frequency control of isolated microgrids. *IEEE Transactions on Smart Grid*, 10(6):6502–6515.

McMahan, H., Moore, E., Ramage, D., Hampson, S., and y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In *AISTATS*.

Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., and Srivastava, G. (2021). Federated learning-based anomaly detection for iot security attacks. *IEEE Internet of Things Journal*, pages 1–1.

Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., and Sadeghi, A. (2019). DÏot: A federated self-learning anomaly detection system for iot. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 756–767.

Nikmehr, N. (2019). Game-theoretic cybersecurity analysis for false data injection attack on networked microgrids. *IET Cyber-Physical Systems: Theory and Applications*, 4:365–373(8).

Oltramari, A., Lebiere, C., Vizenor, L., Zhu, W., and Dipert, R. (2013). Towards a cognitive system for decision support in cyber operations. In *STIDS*.

Pasqualetti, F., Dörfler, F., and Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., and Xu, S. (2016). A survey on systems security metrics. *ACM Comput. Surv.*, 49(4).

Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., and Ilie-Zudor, E. (2018). Chained anomaly detection models for federated learning: An intrusion detection case study. *Applied Sciences*, 8(12).

Saad, W., Han, Z., and Poor, H. V. (2011). Coalitional game theory for cooperative micro-grid distribution networks. In *2011 IEEE International Conference on Communications Workshops (ICC)*, pages 1–5.

Savola, R. M. and Abie, H. (2009). Development of measurable security for a distributed messaging system. In *International Journal on Advances in Security*, pages 358–380.

Shnitko, A. (2003). Adaptive security in complex information systems. In *7th Korea-Russia International Symposium on Science and Technology, Proceedings KORUS 2003. (IEEE Cat. No.03EX737)*, volume 2, pages 206–210 vol.2.

Vu, T. V., L. Nguyen, B. H., Ngo, T. A., Steurer, M., Schoder, K., and Hovsapian, R. (2019). Distributed optimal dynamic state estimation for cyber intrusion detection in networked dc microgrids. In *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, volume 1, pages 4050–4055.

Whitehead, D. E., Owens, K., Gammel, D., and Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, pages 1–8.

Wu, P., Huang, W., Tai, N., and Liang, S. (2018). A novel design of architecture and control for multiple microgrids with hybrid ac/dc connection. *Applied Energy*, 210:1002–1016.

Xu, Q., Ali, S., and Yue, T. (2021). Anomaly detection with digital twin in cyber-physical systems.

Yuan, E. and Malek, S. (2012). A taxonomy and survey of self-protecting software systems. In *Proceedings of the 7th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, SEAMS '12, page 109–118. IEEE Press.

Zhang, H., Meng, W., Qi, J., Wang, X., and Zheng, W. X. (2019). Distributed load sharing under false data injection attack in an inverter-based microgrid. *IEEE Transactions on Industrial Electronics*, 66(2):1543–1551.

Zhao, J., Mili, L., and Wang, M. (2018). A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. *IEEE Transactions on Power Systems*, 33(5):4868–4877.

Zhao, Y., Chen, J., Wu, D., Teng, J., and Yu, S. (2019). Multi-task network anomaly detection using federated learning. In *Proceedings of the Tenth International Symposium on Information and Communication Technology*, SoICT 2019, page 273–279, New York, NY, USA. Association for Computing Machinery.