Cooperative and smart attacks detection systems in 6G-enabled Internet of Things

Hichem Sedjelmaci, Nizar Kheir, Aymen Boudguiga, Nesrine Kaaniche

Cooperative and smart attacks detection systems in 6G-enabled Internet of Things

Hichem Sedjelmaci[1], Nizar Kheir[1], Aymen Boudguiga[2], Nesrine Kaaniche[3]
[1]Ericsson R&D Security, Massy Palaiseau,91120, France
{hichem.sedjelmaci , nizar.kheir}@ericsson.com
[2]Université Paris−Saclay,CEA−List,91120,Palaiseau,France
Aymen.BOUDGUIGA@cea.fr
[3]Telecom SudParis,Polytechnic Institute of Paris,France
kaaniche.nesrine@telecom-sudparis.eu

Abstract

The Sixth Generation (6G) of mobile networks offers the promise of a global interconnected system, serving a large set of applications across multiple fields such as satellite, air, ground, and underwater networks. It will evolve towards a unified network compute fabric that facilitates convergence across ecosystems, fostering design and innovation of new Internet of Things (IoT) applications and services, further leading to an exponential growth of IoT use cases in the post-6G era. This profound evolution will also contribute to further evolving the threat landscape, adding new threat actors, and leading to a new set of cyber security challenges. This paper reviews 6G applications and analyzes their evolved security challenges and existing solutions, covering both the network, application and data layers. It introduces a new concept to security monitoring and attack detection in 6G-enabled IoT systems, leveraging on hierarchical and collaborative approaches, while also satisfying the main 6G's Key Performance Indicators (KPIs) such as trustworthiness, latency, connectivity, data rate and energy consumption. The proposed solution implements a multi-level Federated Learning (FL) approach between IoT devices and edge computing applications. As compared to current centralized security monitoring and detection solutions, it better conciliates between the attack detection accuracy and the network overhead for implementing this model. We demonstrate the use of the proposed solution through an example scenario involving an Internet of Vehicles that communicate over a 6G network.

Keywords—6G, Security scheme, Attacks and KPIs.

I. INTRODUCTION

The Sixth Generation (6G) network is the latest revolution of wireless communications. It provides a fully connected Internet of Things (IoT) and promotes the development of new IoT use cases and applications [1]. To build a global smart connected world, the 6G technology gathers underwater, ground, air and space communication networks. Researchers from industry and academia have already started specifying the first technological building blocks of the 6G architecture as illustrated for instance in these recent works [2, 3, 4]. In [4], Letaief et *al*. introduce a roadmap for 6G deployment and describe a set of AI-enabled use cases such as distributed machine learning for AI-based mobile applications aiming at improving QoS. Gui et *al*., [2] describe four communication services that will be provided by the 6G architecture: Massive Low Latency Machine Type communication (MLLMT), Mobile Broad Bandwidth and Low Latency communication (MBBLL), Massive Broad Bandwidth Machine Type communication (MBBMT) and 6G-Lite. 6G-Lite mainly targets Cooperative Intelligent Transportation Systems (C-ITS). Mao et *al*., [3] highlight the main characteristics of IoT in the context of 6G-enabled IoT applications. They emphasize on various IoT device constraints, usually considered as resource-impoverished in terms of processing and battery capacities, to perform heavy-computational machine learning algorithms or adapt radio resources from high-frequency bands to short-range ones.

Despite the obvious advantages of this new generation of mobile networks, its benefits are often accompanied by new cybersecurity challenges (in the form of new threat actors or new attack surfaces) partly due to the new embedded technologies like for virtualization and adversarial machine learning [5], as well as economic and geopolitical stakes behind this technology and its usages. Therefore, the security of 6G networks, including protection against both external attackers and insiders, will continue to be a major requirement, and a key enabler to accelerate future 6G deployments.

There is a common consensus within the security research community about AI-based security, and the fact of it being a main building block of the 6G architecture [1][2]. These AI-based security systems rely on hybrid detection techniques [6]. They combine conventional detection methods (e.g., signatures-based detection) with more advanced machine learning techniques to capture deviations in the behavior of mobile devices, and further attribute them to either attacks or security breaches. Compared to conventional detection techniques, AI-based misbehavior detection provides both a higher detection accuracy as against unknown zero-day attacks, as well as a reduced false detection rate. In this scope, Federated Learning (FL) is a promising technique that offer to address different 6G security use cases, such as monitoring, attack detection, and orchestration. This is partly due to two reasons: (*i*) the centralized and distributed compute logic, where each device locally executes the FL algorithm and exchange only the hyper-parameters of the learning models, making it even harder to the attacker to tamper with the training data, and also interfere with the learning process, and (*ii*) The distributed and centralized nodes require a low computation overhead as they process only the training models.

While we highlight in this work importance of securing the 6G network, we propose a new security scheme that aims to enhance detection of attacks within 6G-enabled IoT networks. First, we introduce an example of a reference 6G architecture, and present a detailed review of the current cybersecurity concepts currently being studied in the 6G

context. Then, we propose a hierarchical defense scheme based on Federated Learning, and that offers to enhance the ability to monitor and detect network attacks in 6G IoT networks. Finally, we illustrate the use of this approach, and demonstrate its efficiency in the context of a 6G-enabled Internet of Vehicles (IoV) network.

II. ARCHITECTURE OF 6G-ENABLED IOT NETWORK

Further expanding the scope of 5G-enabled use-cases, the 6G architecture will further enhance convergence between heterogeneous networks, including for satellite, air, ground and underwater communication networks [1], as depicted in Figure 1. By integrating satellite and underwater communications (as compared to 5G use-cases), the 6G aims at significantly reducing the latency between the different networks, and more importantly to lay down the ground for new usage scenarios, such as support for a universal device-to-device communication network, increased convergence between the physical and digital universes (also called metaverse), and a far richer set of use-cases in support for new verticals. Below we briefly introduce the scope of each physical network, and the interconnections between the different networks.

- **IoT based air network:** this network encompasses different types of flying devices such as airplanes, Unmanned Aerial Vehicles (UAV), balloons, and helicopters, to cite a few. To achieve global coverage and prevent network outages, the flying devices will co-establish communication links not only together but also with IoT devices deployed in the ground and underwater.

- **IoT based ground network:** the heterogeneous ground network is connecting static and mobile devices such as sensors, actuators, smart meters, vehicles. These devices are connected to the 6G cellular network through TeraHertz (THz) and millimeter Wave (mmWave) communications by using Micro and Nano antennas. In a 6G architecture, the ground IoT devices are aimed to be smarter, and will achieve an efficient Device-to-Device (D2D) communication with a high data rate [1].

- **IoT based underwater network:** the underwater network interconnects a set of heterogeneous underwater devices such as sensors, underwater vehicles and submarines deployed in a wide and deep-sea area. These devices ensure collaborative data analysis tasks. The sonar is considered as the primary communication means to build an underwater cooperative ad-hoc network [1][2].

- **Satellite network:** the satellite network offers a variety of services related to earth observation for weather forecast, system navigation, television broadcasting, *etc*…. In the 6G context, the integration of satellite communication with the air-ground-underwater networks will guarantee an enhancement on data broadcasting and relaying, reliable and seamless services, high quality of service and reliable disaster-recovery communications [7]. China is the first country that deployed a 6G satellite network with the exact purpose of increasing the current 5G broadcast speed by 100.

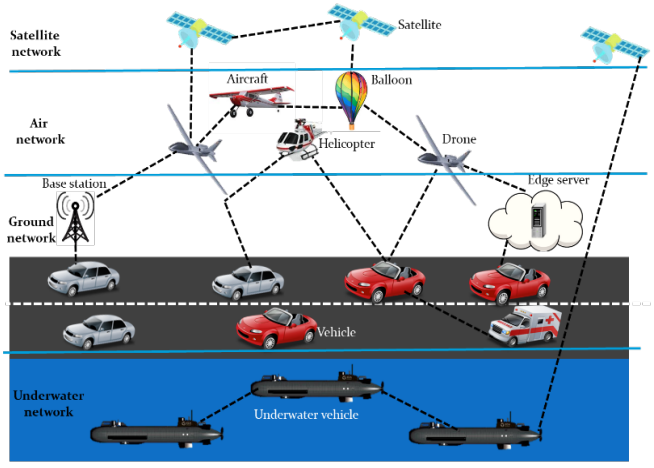


Figure 1. Architecture of 6G-enabled IoT network.

III. CYBER SECURITY IN 6G WIRELESS NETWORKS

In this section, we review the current security mechanisms that are designed to ensure security and privacy properties and protect the future 6G architecture from common cyber-attacks. In the following, we present different approaches at the application and the infrastructure levels:

A. Application and data levels

Li et al. [1] proposed a cyber protection scheme that relies on blockchain technology to ensure communication security in a 6G-enbaled IoT network. The protection scheme is based on four entities: an edge server, a public blockchain platform, a central authority and distributed devices. These entities cooperate together to protect the exchanged data from the malicious IoT users. The blockchain relies on a reputation algorithm, where each IoT device has a reputation value determined according to its normal and malicious behaviors. Their proposed solution protects against tampering threats where an attacker aims at modifying the reputation score. Mousa *et al.* [8] conceived a lightweight authentication protocol based on a public key encryption scheme and adapted to heterogeneous wireless networks, such as a 6G network. The authentication process is performed between a base station and the devices that store the encryption keys. In their analysis, Mousa *et al.* claim that their authentication scheme is secure against common attacks, namely replay, spoofing and man-in-the-middle attacks, while being simple and easy to implement compared to blockchain-based solutions. Li *et al.* [9] addressed the data confidentiality requirement in 6G wireless communications through the implementation of a caching system and the deployment of a physical layer security mechanism. They proposed a secure probabilistic model based on a probability caching and redundancy rate to secure the 6G transmission links against the eavesdropping attacks. Their simulations showed acceptable performance results in terms of secure transmission rates as compared to previous works. Although the aforementioned solutions [1, 8, 9] are secure against external attackers, they fail to detect internal adversaries, such as malicious base stations or infected edge servers.

B. Infrastructure level

Stergiou *et al*. [10] developed a data management protocol for 6G networks. They designed a cache decision system that operates over a smart building to help end-users browse the Internet, share and manage large-scale data. The proposed decision system is proven secure against internal and external attacks. It relies on two main servers, namely an edge and a cloud server that collaborate to monitor the traffic and to detect attacks, while taking into account the network latency and energy consumption. However, the authors do not evaluate the performances of their proposed mechanism against attacks that could target the 6G network. In [11], Li *et al.* studied the application of Federated Learning (FL) in the context of a 6G architecture. Specifically, they used a secure FL approach to thwart attacks targeting the wireless communication and machine learning-based algorithms. They analyzed three FL defense strategies, namely a detection mechanism, a reputation management algorithm and an aggregation scheme. However, the authors do not provide an experimental analysis of the proposed FL defense strategies in terms of accuracy, robustness and efficiency. Mao *et al.* [3] proposed an AI-based security system based on Kalman filtering to protect the low-resource IoT devices from the attackers that target the energy consumption of the legitimate entities. The main purpose of this work is to ensure a tradeoff between the quality of service and the security in the context of 6G network. According to their experimental results, the authors proved that their proposed solution achieved a high level of security and it is adapted for energy-constrained devices. However, the authors do not perform an experimental analysis of their security system against the well-known attacks targeting the constrained IoT network such as resource exhaustion attacks.

Table I presents a comparison between the aforementioned solutions in terms of functional properties, security properties and Key Performance Indicators (KPIs). Among the 6G's KPIs we consider:

- *Energy consumption*: this KPI mainly focuses on evaluating the energy consumption rate of resource-constrained devices of the network. Indeed, the resource exhaustion attacks target the resource-limited devices of the network (such as sensors and drones). The attack consists of forcing the legitimate IoT devices to carry out further computation and communication tasks and hence decrease promptly their lifetime by exhausting their batteries.

- *Connectivity:* the tactile IoT is considered as one of the main MBBMT services and it requires a massive connectivity for the large-scale deployed devices to exchange the gathered and processed data in an efficient manner [2]. To enhance the quality of connectivity in 6G-enabled IoT networks, one major technical challenge is improving the positioning accuracy, specifically for mobile IoT devices as explained in [2]. For instance, the GPS spoofing is considered as one of the critical cyber threats that target the positioning accuracy of mobile devices, by altering their GPS coordinates. The Signal Strength Intensities (SSIs) generated by the monitored devices is defined by security experts as the main feature that should be monitored to detect GPS spoofing [12].

- *Latency:* this KPI is considered as a main metric of 6G-Lite scenarios, such as intelligent transportation systems. Here, malicious entities compel legitimate IoT devices or edge servers to run unnecessary computation tasks leading to an increase of the network latency.

- *Data rate:* almost all of MBBLL applications, e.g., augmented and virtual reality, require high data rate and low latency in order to achieve high-definition video transmission as discussed in [2]. The Denial of Service (DoS) attacks could drop the relevant packets and hence decrease the data rate or/and send a huge number of unwanted packets, thus impacting the network latency.

TABLE I. COMPARISON BETWEEN CYBERSECURITY SOLUTIONS FOR 6G-ENABLED IOT APPLICATIONS

Solution	Approach	Internal attacks	External attacks	Accuracy of attacks detection	Energy consumption	Connectivity	Latency	Data rate
[1]	Blockchain	Non detectable	Detectable	Medium	High	Medium	High	NA
[9]	Cryptographic-based solution	Non detectable	Detectable	Medium	High	Medium	Low	NA
[8]	Caching system	Non detectable	Detectable	Medium	NA	NA	High	NA
[10]	Caching decision system	Detectable	Detectable	Medium	Medium	Medium	Low	High
[11]	Federated Learning (FL)	Detectable	Detectable	NA	NA	High	Low	High
[3]	Kalman filtering	NA	Detectable	High	Medium	NA	Low	High
Proposal	Hierarchical FL	Detectable	Detectable	High	Medium	Medium	Low	High

IV. HIERARCHICAL FEDERATED LEARNING SECURITY SCHEME FOR 6G-ENABLED IOT NETWORKS

We introduce in this section a new concept for security monitoring in 6G networks. The new concept aims to achieve a high level of resilience against insider and outsider attacks (e.g., attackers compromising or hijacking distributed security agents in the network), as well as a higher efficiency for threat detection and diagnosis. This concept leverages on hierarchical Federated Learning. It fosters a collaborative approach for security monitoring where decentralized agents are trained to detect attacks in the 6G network and further exchange the learnt model without exposing real data. Such decentralized approach would contribute to reducing the network overhead (due to the sharing of real-time data) and provide better privacy assurance as the monitored data (both control and user plane data) never leaves the local processing node.

A. Overview

The proposed security scheme involves three entities, namely the distributed IoT nodes, the edge servers, and the Security Information and Event Management (SIEM). Those entities contribute to implementing and operating a hierarchical Federated Learning approach for security monitoring, all contributing to the Federated Learning process, as shown in Figure 2. They collaborate together to detect common attacks against the 6G network, as follows:

-Distributed IoT nodes: We distinguish two types of IoT nodes Cluster Head (CH) and Cluster Member (CM) nodes. The election of the CH node depends on its Maliciousness Level (ML) and the network requirements of the 6G-enabled IoT network summarized by the aforementioned KPIs. KPIs

define latency, data rate, connectivity and energy consumption levels that a node must satisfy to be selected as a CH [1][2]. The CH monitors the behaviors of its CM nodes by applying intrusion detection techniques based on a FL algorithm, which will be explained in the *hierarchical FL-Security framework paragraph below*. Indeed, when an attack is detected at a CM level, the CH sends an *Alert message* to the edge server, which in turn forwards it to SIEM for further analysis. The *Alert message* includes the identity of the suspected node, and the values of ML and 6G network's KPIs that the suspected node exhibits. It is noted that, the CM monitors the CH by applying a signature-based attacks detection.

-***Edge server:*** It has a powerful computation capability and a mass storage capacity that are used to analyze the huge amount of data and *Alert messages* received from the IoT nodes. The FL algorithm is used as a detection technique to verify the malicious behaviors of suspected CM nodes, detected by the CH nodes. The edge server analyzes the behavior of CHs (that are located within the edge server's range) with a goal to determine the malicious CH nodes. Then, the edge server sends a *Report message* including the identity of suspected nodes (CMs or/and CHs) and their KPIs to the SIEM for further analysis and decision making regarding suspected CM or CH as malicious.

-***SIEM*:** It is a centralized cloud server that manages the distributed edge servers deployed within the 6G-enabled IoT network. SIEM carries out the correlation and detection process to determine the malicious IoT devices with a high accuracy. In the correlation process, SIEM aggregates the relevant information extracted from *Report* and *Alert messages* to generate a global *Report message,* which includes the updated values of ML and 6G network's KPIs related to each monitored IoT node. In the detection process, the FL algorithm is used to analyze the behaviors of monitored targets to detect the misbehaving edge server, and malicious CM and CH devices.

-***Hierarchical FL-security framework:*** A FL-based attacks detection approach is used to identify the malicious IoT devices. These malicious devices strive to decrease the quality of service by impacting the main KPIs of the 6G network, as explained in the attacker model section below. As shown in Figure 2, the hierarchical FL algorithm is performed at the IoT and edge levels.

In the IoT level, the FL algorithm is divided into three phases: the clustering, the training and the detection phases. During the clustering phase, a set of secure IoT clusters is created with respect to the network requirements of 6G architecture, as explained in the case study section. At each cluster, the trusted CH device joins the nearest edge server for sharing the training models and all attacks' detection events. During the training phase, each edge server sends to its respective CH devices the pre-trained global models, denoted w_t^i, where $i = \{1, \dots, K\}$ and K is the number of edge servers. The CH device uses its local data sets and trains the global model w_t^i to obtain the updated global training model w_{t+1}^j, where $j = \{1, \dots, K'\}$ and K' is the number of CH devices. Each CH uploads the updated model w_{t+1}^j to its respective edge server and this latter aggregates all the received models w_{t+1}^j to obtain the new global model w_{t+1}^i. The CH devices download from their edge server the latest global model w_{t+1}^j. In the detection phase, the CHs and edge server categorize the behaviors of their respective monitored devices, CMs and CHs either as normal or as malicious according to the global training model obtained during the training process. As indicated above, in case of detected attacks, the *Alert* and *Report messages* are forwarded to SIEM for further analysis.

The execution of the FL algorithm at the edge level is divided into two phases: the training and the detection/decision phases. The process of training is similar to the one performed at the IoT level, where the goal is to determine a general model w_{t+1} shared between the edge servers and the SIEM. In the detection/decision phase, the SIEM monitors the behaviors of edge servers and analyzes the information extracted from the *Alert* and *Report* messages to verify whether the suspected CH or CM device is malicious. The security experts validate the SIEM decisions. Indeed, the experts append relevant security data and update the SIEM by adding new attacks features. As such, they improve the training process and hence increase and decrease the attacks detection and false detection rates, respectively.

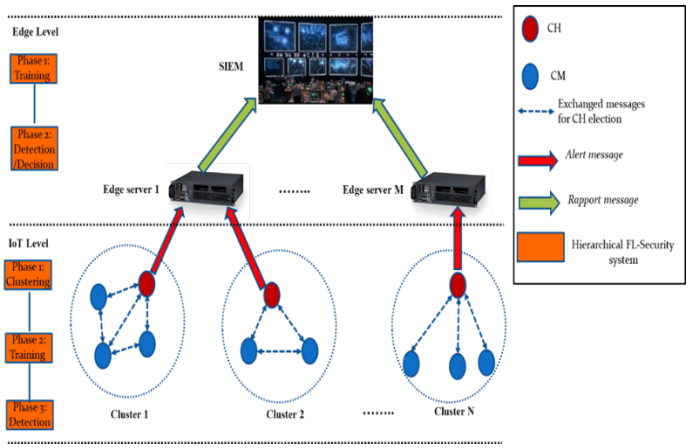


Figure 2. Hierarchical FL-based defense architecture

B. *Attacker model*

For the attacker model, we consider two main types of adversaries defined as follows:

-*External adversaries*: include malicious entities that seek to hijack main security properties such as data confidentiality or integrity, as well as network service availability. They may also include other form of attacks, such as the one aiming to deteriorate the featured 6G KPIs, such as to increase latency, to exhaust network resources, generate overhead, or increase the energy footprint (e.g. altering the signal strength intensities). Note that data that is relevant to each KPI defined above, i.e., energy consumption, Signal Strength Intensities (SSIs), computation and communications overheads, and data rate can be used by the agent as input for executing the Federated Learning approach and for attack detection. Similarly, other 6G's KPIs such as capacity and bandwidth consumption can be monitored in the same way, to train the system so as to detect other kinds of attacks, including examples like distributed botnet and aggressive fuzzing.

-*Internal adversaries*: include malicious IoT devices and malicious edge servers that could target the hierarchical FL-security system by modifying the training vectors and hence altering the trainings models (w_{t+1}^j, w_{t+1}) of FL algorithms (these are also referred to as poisoning attacks against the distributed security monitoring framework). The current state of the art already provides solutions how to limit the effect of

poisoning attacks, as in [11][13] where the authors proposed a security solutions that leverage on aggregation and reputation algorithms to evaluate the information sent by the cooperative nodes executing the FL algorithms. In the context of future 6G networks, the collaborative nodes mainly refer to the three acting entities that execute the Federated Learning process, which are the distributed IoT nodes, the edge servers, and the security orchestration framework(as SIEM).

C. Case study: Securing IoV network in 6G-Lite

The Internet of Vehicles (IoV) network is considered as one of the main 6G-enabled IoT networks adapted for 6G-Lite. The 6G-enabled IoV network involves several heterogeneous mobile devices, e.g., automotive vehicles, drones and underwater vehicles as shown in Figure 1, that are particularly distinguished by the high mobility characteristic. This makes significant the assurance of high data rate, low latency and massive connectivity indicators [2]. The IoV network is based on a clustering architecture, where mobile devices that are located within the same radio range are organized into a one-hop cluster, as depicted in Figure 2. The election of the CH device of a particular cluster depends on its Maliciousness Level (ML) and the agreed 6G's KPIs that the elected CH should satisfy, defined as follows:

-*ML:* Before clusters creations, each IoV node monitors its neighboring devices by executing signature-based attacks detection technique. Indeed, it assigns ML values to monitored devices, where ML should increase or decrease with respect to their normal or suspicious behaviors. The neighboring IoV devices exchange periodically the computed MLs related to the monitored neighboring devices. After cluster formation, each CH is running the anomaly detection model trained using FL and assigns MLs to its CM. For more details on how to compute the ML in a cluster based secure IoV network, we refer the reader to reference [14]. MLs are computed using authentic data which are securely exchanged after mutual authentication between the different devices. The choices of the authentication protocol and the encryption algorithm are out of scope.

-*Latency*: the neighboring IoV devices exchange periodically the required computation time (in m/s) for running specific tasks such as the model training and misbehavior detection.

-*Connectivity degree:* it refers to the number of IoV devices (CMs) and edge servers connected to the candidate CH. The connectivity degree related to each monitored IoV device is periodically exchanged among the neighboring mobile devices.

-*Data rate*: it corresponds to the maximum number of bits per second that the IoV device can disseminate. Each IoV device broadcasts the value of its data rate to its neighboring devices.

-*Energy consumption:* each resource constrained IoV device such as UAV broadcasts periodically the value of its remaining energy to its neighboring IoV devices.

The IoV device that is elected as a CH is the node with the lowest ML and which ensures a network tradeoff between low latency, high connectivity, high data rate and low energy consumption (when the CH candidate is an UAV). Here, ensuring the network tradeoff means that the elected CH should satisfy at least one requirement of the aforementioned 6G's KPIs. For instance, the latency of the elected CH might be lower than its CMs or/and the connectivity degree of the elected CH is higher than its CMs, *etc.* After the CHs election at each cluster, the CH devices and their respective CMs monitor mutually their behaviors by running the FL algorithm and signature-based detection, respectively. When the ML of CH is higher than its CMs or/and this CH does not ensure a network tradeoff of 6G's KPIs requirements; one of the CMs is elected as a new CH.

D. Simulation results

For our experiments, we simulate a set of distributed nodes that simulate individual devices with an IoV network (e.g., Ground vehicles, Drones and Underwater vehicles), where a total number of 40 nodes are deployed within the network. One of the use cases that the cooperative IoV nodes could perform is the search and rescue operations of vulnerable entities located in the distressed vessels and aircrafts. At the beginning of our simulation, for each IoV node, we fix the values of latency, connectivity degree, data rate and energy consumption. Then these values will be changed randomly over time. The federated learning setup is configured as follow: learning rate = 0.5, maximum number of iteration =50 and batches sizes of CH, edge server and SIEM = (5, 30, 60). We use a fully connected feed-forward neural network with 40 input neurons, where the network is trained with cross entropy loss. To conduct the different experiments, we consider the major attacks that target the wireless communication, relying on the attacks dataset, introduced in [15]. The latter serves to assess the performance evaluation of the proposed hierarchical security scheme. This dataset corresponds to the real cyber-threats against the IoT devices and edge networks; where these cyber-threats may be performed against the radio access of 5G and 6G networks.

For our analysis, we define a new metric called *secure IoV4_6G*. It is computed as the ratio of the number of secure and efficient IoV clusters with respect to the total number of IoV clusters. The secure and efficient IoV clusters correspond to the trusted IoV clusters (i.e., their CHs have lowest MLs) that satisfy the requirements of 6G's KPIs. As shown in Figure 3, after cluster formation we vary the number of iterations from 5 to 50 iterations: at each iteration, the hierarchical FL algorithm is run at both IoT devices and edger servers and covers the training and the detection/decision phases as explained in *hierarchical FL-security framework*. From Figure 3, it is clear that when the number of iterations increases the *secure IoV4_6G* metric improves, specifically when the number of iterations is equal to 50. This result is attributed mainly to the following reasons: (*i*) hybrid detection and mitigation: by combining between signature-based detection and FL based attacks detection techniques the CH and its CMs monitor mutually their behaviors; and also each CM monitors its CM neighbors by using signature detection technique. Furthermore, each edge server monitors the behavior of its CHs by using the FL algorithm. (*ii*) Tradeoff between the network and security constraints: as explained in the case study subsection, creation of IoV clusters is based mainly on ensuring a high number of secure clusters, while taking into account the main requirements of 6G's KPIs such as latency, connectivity and data rate.

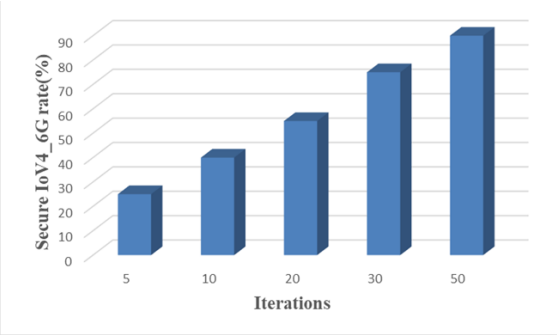
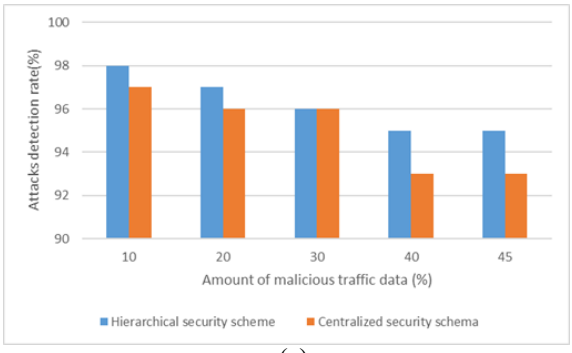
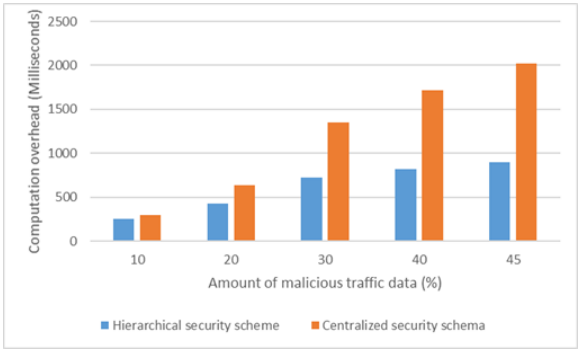


Figure 3. Security IoV4_6G rate of the proposed hierarchical security scheme.

In Figure 4, the proposed hierarchical security scheme is compared to the centralized security schemes such as [9][10], where in these centralized schemes the cyber protection, attacks detection and mitigation processes are performed in centralized nodes such as edge servers. Here, the attack detection rate and computation overhead are evaluated. As shown in Figure 4.(a), the detection rate of attacks targeting the IoT devices and edge servers is high for the hierarchical and centralized security schemes since for both security schemes almost of attacks occurring within the edges 'range are detected with a high accuracy, specifically when the number of iterations is high. However, as shown in Figure 4. (b), the computation overhead generated by the centralized security scheme is high since in a centralized scheme a huge amount of data is processed in a centralized node (i.e., edge server) to prevent the external and internal attacks on executing cyber threats. In a hierarchical scheme the generated computation overhead is less since to lighten the cyber defense process (i.e., attacks detection and mitigation process) at the edge server (and SIEM), three defense layers are used to secure the network, which are executed at IoT device and edge levels.



(a)



(b)

Figure 4. Hierarchical and centralized security schemes: a) attacks detection rate; b) computation overhead.

V. Conclusion

The implementation of 6G ultra-dense and heterogeneous networks, applications and services is drawing the attention of IT and telecommunication companies. However, the deployment of efficient security mechanisms in the context of 6G architectures has yet to be explored. In this research work, we have proposed a new collaborative cyber security system, based on a multi-level FL algorithm, to secure 6G-enabled heterogeneous IoT networks from attacks targeting the main KPIs of 6G architectures. To the best of our knowledge, we are the first to propose a concrete construction of a hierarchical defense system run by IoT nodes, edge server and SIEM, in the context of 6G networks. The proposed solution is a new step in the research and development of cybersecurity mechanisms and machine learning algorithms in emerging 6G-enabled IoT networks, and will be beneficial to the scientific and industrial communities.

References

[1] W. Li, Z. Su, R. Li, K. Zhang, Y. Wang, "Blockchain-Based Data Security for Artificial Intelligence Applications in 6G Networks", *IEEE Network*, Vol 34, Issue 6, pp. 31-37, 2020.

[2] G. Gui, M. Liu, F. Tang, N. Kato, F. Adachi, "6G: Opening New Horizons for Integration of Comfort, Security, and Intelligence", *IEEE Wireless Communications*, Vol 27, Issue 5, pp. 126-132, 2020.

[3] B. Mao, Y. Kawamoto, N. Kato, "AI-Based Joint Optimization of QoS and Security for 6G Energy Harvesting Internet of Things", *IEEE Internet of Things Journal*, Vol 7, Issue 8, pp. 7032 - 7042, 2020.

[4] K-B. Letaief, W. Chen, Y. Shi, J. Zhang, Y-J-A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks", *IEEE Communications Magazine*, Vol 57, Issue 8, pp.84-90, 2019.

[5] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, "Security and privacy in 6G networks: New areas and new challenges", *Digital Communications and Networks*, Vol 6, Issue 3, pp. 281-291, 2020.

[6]S. Kaur, M. Singh, "Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks", *Neural Computing and Applications,* Vol 32, pp.7859–7877, 2020.

[7] M. Giordani, M. Zorzi, "Satellite Communication at Millimeter Waves:a Key Enabler of the 6G Era", *IEEE International Conference on Computing, Networking and Communications (ICNC)*, Big Island, HI, USA, 2020.

[8] A. Al Mousa, M-A. Qomri, S-A. Hajri, R. Zagrouba, "Utilizing the eSIM for Public Key Cryptography: a Network Security Solution for 6G", *IEEE 2nd International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2020.

[9] S. Li, W. Sun, H. Zhang, Y. Zhang, "Physical Layer Security for Edge Caching in 6G Networks", *IEEE Global Communications Conference*, Taipei, Taiwan, 2020.

[10] C-L. Stergiou, K-E. Psannis, B-B. Gupta, "IoT-based Big Data secure management in the Fog over a 6G Wireless Network", *IEEE Internet of Things Journal*, Vol 8, Issue 7, pp. 5164 – 5171, 2020.

[11] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, D. Niyato, "Federated Learning for 6G Communications: Challenges, Methods, and Future Directions", *China Communications*, Vol 17, Issue 9, pp. 105-118, 2020.

[12] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal and J. Fagan, "Countermeasures for GPS signal spoofing", *Proc. 18th Int. Tech. Meeting Satellite Div. Inst. Navig.*, pp. 1285-1290, 2005.

[13] J. Kang, Z. Xiong, D. Niyato, Y, Zou, Y. Zhang, M. Guizani, "Reliable Federated Learning for Mobile Networks", *IEEE Wireless Communications*, Vol 27, Issue 2, pp. 72-80, 2020.

[14] H. Sedjelmaci, S-M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks", *Computers & Electrical Engineering,* Vol 43, 2015, pp. 33- 47.

[15] M. Nour, J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)", *IEEE Military Communications and Information Systems Conference*, Canberra, ACT, Australia, 2015.