Multi-process Federated Learning with Stacking for Securing 6G-V2X Network Slicing at Cross-Borders

Abdelwahab Boualouache, *Member*, *IEEE*, Amirhossein Adavoudi Jolfaei and Thomas Engel, *Member*, *IEEE*

Abstract—Being part of the 6G ecosystem vision, Connected and Automated Vehicles (CAVs) will enjoy sophisticated tailored services offering road safety and entertainment for users. As one of the 6G cornerstones, Network Slicing (NS) allows the creation of various customized 6G-V2X (Vehicle-to-Everything) use cases on the same physical infrastructure. However, 6G-NS advances can open up breaches to cyber-attacks aiming to break 6G-V2X Network slices to inflict maximum damage on CAVs and their users. Crossing borders, where CAVs leave their V2X-NS (V2X Network Slice) in the Home Mobile Network Operator (H-MNO) toward a similar V2X-NS in the Visited MNO (V-MNO), is an attractive opportunity to exploit by attackers. Detecting and mitigating attacks, in this case, becomes a priority, confronted by NS requirements and MNOs not ready to share their private data. To this end, this paper proposes a 3GPP-compliant privacy preservation collaborative learning scheme for 6G-NS security, focusing on V2X-NS cross-border areas. Our scheme leverages multi-process Federated Learning (FL) architecture to build efficient V2X-NS security-related models while preserving 6G V2X-NS isolation. In addition, it uses differential privacy-enabled stacking to build up attack detection knowledge at the V2X-NSs and MNOs levels while ensuring privacy preservation. We conducted an experimental study on the 5G-NIDD dataset, which is one of the most realistic publicly available 5G datasets. Our results demonstrate that multi-process FL with stacking can deliver high accuracy while ensuring isolation between 6G-V2X-NSs and privacy preservation between H-MNO and V-MNO.

Index Terms—6G-V2X; Network Slicing; Security; Machine learning; Misbehaving Detection Systems, Federated learning

1 Introduction

The success of the 5th generation of mobile networks (5G) in integrating innovative verticals with various requirements under a unified communication framework has paved the way for the following mobile generation. 6G will enforce 5G-enabling technologies and continue the development of AI-empowering and fully-automated solutions [1]. Advanced Network Slicing (NS) is one of the cornerstones of 6G ecosystems, enabling several verticals and use cases with stringent network and security requirements to co-exist in the same environment while sharing the same physical infrastructure [2]. However, 6G-NS will face a massive vector of cyberattacks from tactical adversaries continuously exploring weak points to break 6G network slices [3].

Connected and Automated Vehicles (CAVs) are critical verticals exploiting 6G-V2X direct communications via PC5 interface and 6G-V2X-NS to deliver reliable and efficient road safety services [4]. Various 6G-V2X Network Slices (6G-V2X-NSs) tailored to specified V2X applications, services, and use cases with different purposes and requirements can be requested by stakeholders (6G-V2X slice tenants), such as road authorities, companies, and content publishers. For example, road authorities can request the creation of a 6G-V2X-NS dedicated to fully automated (autonomous) vehicles requiring ultra-reliable communications. In addition, companies can request creating a dedicated 6G-V2X-NS for their delivery/supply-chain platoons while ensuring platoon stability. Media publishing can request a 6G-V2X-NS to broadcast relevant content to the CAV's passengers.

However, CAVs are attractive targets to adversaries who aim to harm end-users, making noise that may cause them to lose trust in 6G. An example of these impacts is recently demonstrated in Denmark, where a cyberattack caused trains to stop [5]. Moreover, mobility CAVs will facilitate adversaries' tasks in breaking 6G-V2X-NSs. Indeed, CAVs moving on roads can perform frequent handovers and may cross borders in open-border geographic areas like Schengen space. Crossing boarding and roaming operations change attachment from the Home Mobile Network Operator (H-MNO) to a Visited MNO (V-MNO). In this case, the V-MNO should allocate a 6G-V2X-NS with the same characteristics as the home 6G-V2X-NS. This will open up several breaches to break [6, 7].

While the current 3rd Generation Partnership Project (3GPP) standard provides roaming security solutions for control and data planes [8], security challenges are higher in 6G-V2X-NSs at cross-borders. Detecting cross-border attacks required cooperation between H-MNO and V-MNO in training Machine Learning(ML)-based security-related models while facing three main challenges (i) the first challenge is to develop ML models for securing 6G-V2X-NSs while ensuring that their respective networks and data remain isolated from each other during the training process, (ii)

A. Boualouache, A Jolfaei, and T. Engel are with the Faculty of Science, Technology and Medicine (FSTM) at the University of Luxembourg, Esch-sur-Alzette, AVE, 4365, Luxembourg. E-mail: {abdelwahab.boualouache,amirhossein.adavoudi, thomas.engel}@uni.lu

H-MNO and V-MNO belong to different countries; thus, they are under different privacy regulations and policies embedding them to share their security and network data for training mutually. Specifically, each country's telecommunications national regulatory authority (TNRA) manages policies and regulations that directly impact security. Therefore, the challenge is to ensure collaboration between H-MNO and V-MNO to detect attacks with adequate accuracy while ensuring privacy preservation (iii) the third challenge is that the proposed collaborative learning security architecture for 6G-V2X-NSs should comply with 3GPP standards.

To address these challenges, we extend 3GPP security roaming standards for securing NS for 6G-V2X, especially in cross-border areas. We proposed a scheme using multi-process Federated Learning (FL) to train 6G-V2X-NS security-related models independently for preserving NS isolation. The scheme offers two strategies for selecting the global MNO models. Finally, it also uses differential privacy-enabled stacking to build collaborative global deep-learning models to detect slicing attacks with adequate accuracy while preserving privacy.

The contributions of this paper can be summarized as follows:

- We propose a security architecture compliant with the 3GPP release 17, exploiting a hierarchical structure of multiple Network Data Analytics Functions (NWDAFs) for the collaborative building of a security model for 6G-V2X-NSs while respecting the requirements.
- We propose multi-process FL for building security-related 6G-V2X models with two strategies for realizing the global model for each MNO.
- We propose differential privacy-enabled stacking for combining global models built at each MNO for building up meta-learner and accumulating detection capabilities while preserving the privacy of each MNO.
- We evaluate the accuracy of our scheme on the 5G-NIDD dataset, which contains attack traces from a realistic 5G testbed, and qualify the impact of differential privacy.

The remainder of this paper is organized as follows. Section 2 discusses the related work. Section 3 describes the system model. Section 4 describes the adversary model. Section 5 presents the building blocks of our scheme. Section 6 describes our experimental setup and obtained results. Section 7 discusses results and some future perspectives. Section 8 concludes the paper.

2 Related work

Research communities have already identified attacks against NS in 5G. The Next Generation Mobile Networks (NGMN) Alliance document [9] has identified early vulnerabilities in 5G NS and given recommendations. However, the attacks on NS have kept developing. The authors of [10] have explored a distributed slice mobility attack that exploits the user equipment-initiated inter-slice mobility, causing performance and economic damage to the 5G network slices. The authors of [11] focused on security threats in 5G-V2X network slices from multiple perspectives, namely CAVs and the underlying network slicing technologies and procedures. The authors of [12] surveyed many ML-based intrusion detection systems for CAVs, highlighting the threats from network slicing and the need to develop similar systems for detecting such attacks. The authors of [13] developed a Deep-Learning (DL) model to select suitable network slices and proactively prevent Distributed Denial of Service attack (DDoS) attacks on a 5G network based on the incoming network connections before they even reach the core network. The authors of [14] proposed a framework based on a Long Short Term Memory DL technique that detects user equipment (UE) network traffic as a DDoS or normal traffic and assigns an appropriate slice to a legitimate UE request. The authors of [15] have developed a DL module to detect DDoS attacks, automatically creating a sinkhole-type slice with a small portion of physical resources and isolating the malicious users within this slice to mitigate the attackers' action. The authors of [16] proposed an FL-based architecture that coordinates security orchestration to centrally handle security operations of network slicing while preserving data privacy. However, the previous works [13–15] have only focused on attacks on the 5G-Core focusing DoS attacks, and without considering 5G-V2X verticals. The authors of [17] have categorized attacks against network slicing into intra-slice and inter-slice attacks. Specifically, intra-slice attacks in which the attacker(s) and the target(s) belong to the same V2X Network Slice (V2X-NS), while inter-slice attacks in which the attacker(s) and/or the target(s) belong to different V2X-NSs. The authors in [18] proposed a DL-based approach to detect V2X network slicing attacks, such as end-to-end from vehicles to the core network. However, the paper only focuses on intra-slice V2X attacks and does not consider inter-slice. The authors in [19] proposed an FL approach to detecting inter-slice V2X attacks. The proposed scheme is hierarchical and deploys a set of DL-empowered security Virtual Network Functions (sVNFs) over V2X-NSs as FL clients and FL coordinators. However, this scheme focuses on detecting the slice inside one MNO and does not consider roaming and cross-border areas. In addition, unlike [19], this paper uses multi-process FL to build multiple ML models for V2X network slices and then combines them to have a single global model for the MNO. Then, this paper builds ML models tailored for cross-border areas by combining global models from the interconnecting MNOs. The authors of [7] have recently identified a set of threats on CAVs at cross borders. Table 1 presents a comparative analysis between related work and our proposed scheme. This comparison is based on five criteria ″V2X″, ″Attack detection″, ″Network slicing″, ″Cross-border″, and ″Privacy Preservation″. As we can see in this table, unlike all the previous works, our scheme focuses on detecting 6G-V2X network slicing attacks in cross-border areas. It proposes collaborative learning based on federated and ensemble learning while considering slice isolation and privacy preservation. Specifically, unlike [16, 19], our scheme leverages multi-process federated learning and complies with the current 5G standards and promises for 6G networks. Table 2 describes the frequent abbreviations used in the paper.

TABLE 1: Comparison table

Scheme	V2X	ML-based Attack detection	Network Slicing	Cross-border	Privacy Preservation
[13]		X	X		
[14]		X	X		
[15]		X	X		
[16]		X	X		X (FL)
[18]	X	X	X		
[19]	X	X	X		X (FL)
Our scheme	X	X	X	X	X (Multi-process FL)

TABLE 2: Abbreviations used throughout the paper.

Abbr	**Description**
3GPP	The 3rd Generation Partnership Project
6G	The 6th generation mobile network
6G-V2X-NS	6G-V2X Network Slices
CAV	Connected and Automated Vehicle
DDoS	Distributed Denial of Service
DL	Deep Learning
ETSI	European Telecommunications Standards Institute
FL	Federated learning
MEC	Machine Learning
MEC	Multi-access Edge Computing
MNO	Mobile Network Operator
NS	Network Slicing
NWDAF	Network Data Analytics Function
SMF	Session Management Function
UPF	User Plane Function

3 System Model

This section describes the system model considered by our scheme. Figure 1 illustrates a cross-border 6G-V2X NS architecture scenario. The main parties of the architecture are the H-MNO and the V-MNO. Each MNO consists of a 6G cloud-native core network, Multi-access Edge Computing (MEC) layer, and New Radio (NR), including CAVs, Vulnerable Road Users (VRUs) (e.g., pedestrians, cyclists, motorcycle riders), and gNodeBs. More specifically, we refer here to a Public Land Mobile Network (PLMN), a combination of wireless communication services offered by a specific MNO in a specific country. The home and visited MNOs are interconnected through N9 and N32 are 6G standards reference points. Specifically, the N32 connects the 6G core networks (visited and home) at the control plane, and N9 allows connection between the V-MNO and H-MNO at the data plane level.

Two strategies are provided by 6G to manage the data session of CAVs. In the Local Break Out (LBO) strategy, only the Visited MNO manages data sessions using the visited User Plane Function (V-UPF) and Visited Session Management Function (V-SMF). In contrast, in the Home-Routed (HR) strategy, the data is routed to the H-MNO, which manages data sessions. Although specified by the 3GPP, the LBO architecture is rarely used in practice [20]. For this reason, our scenario adopts HR architecture. For example, in our scenario, 6G-V2X application data is routed from the H-MNO to the V-MNO first through the N4 interface and then through the N9 interface between H-UPF and V-UPF.

6G-V2X-NSs are created and managed by the Network Slice Manager (NSM) upon establishing a Service Level Agreement (SLA) between the tenant (the stakeholder) and the MNO. The MNO should ensure the security of the 6G-V2X-NS and the service continuity even after crossing the borders. Moreover, different isolation levels could exist between the 6G-V2X-NSs, ranging from complete isolation, where each 6G-V2X-NS has its own Cloud Native Functions (CNFs), to partial isolation, where 6G-V2X-NSs share few or several CNFs. Our scenario, illustrated in Figure 1, adopts 6G-V2X-NS isolation at the data plane. More specifically, 6G-V2X-NS share 6G-Core control CNFs, and each 6G-V2X network slice has a dedicated UPF. This function is usually placed close to the users at the MEC layer to provide better performance [21].

Three strategies can be applied to ensure the continuity of 6G-V2X slice services [22]: (i) the V-MNO provides a 6G-V2X-NS with equivalent functionality of the V2X-NS used in the H-MNO, (ii) the H-MNO can export the blueprint of 6G-V2X-NS to the V-MNO, so the latter can instantiate a similar V2X-NS administrated by it, and (iii) the H-MNO can extend the 6G-V2X-NS into the V-MNO and provide it with authorization to control the resources. In the real-world scenario, it is up to the V-MNO to determine the best strategy to ensure service continuity service. The first strategy seems more realistic for the standardized types of 6G-V2X-NSs. Therefore, when registering to the V-MNO, V2X nodes can be mapped to 6G-V2X-NS, meeting the same requirements as V2X-NS of the H-MNO [20].

From a security perspective, the cross-border scenario differed from the general multi-MNO scenario since H-MNO and V-MNO are under different policies and regulations. For example, policies and regulations regarding certain tools and technologies and data processing procedures can embed the V-MNO to provide the same security level for the 6G-V2X-NS as at the H-MNO [7]. Therefore, in the cross-border scenario (international roaming), the interconnecting MNOs should harmonize their different-level security solutions to meet the hosting countries' policies and regulations while maintaining the security of 6G-V2X during roaming, which is not easy and requires cooperation between the H-MNO and home V-MNO.

The current 3GPP standard proposes a Security Edge Protection Proxy (SEPP) at the edge of the core network to protect control plane exchange through the N32 interface, providing security features such as topology hiding, message filtering, and many other policy enforcement capacities. The SEPPs of H-MNO and V-MNO communicate through the Internet Protocol Exchanges and have Transport Layer Security (TLS) as the authentication protocol. How-

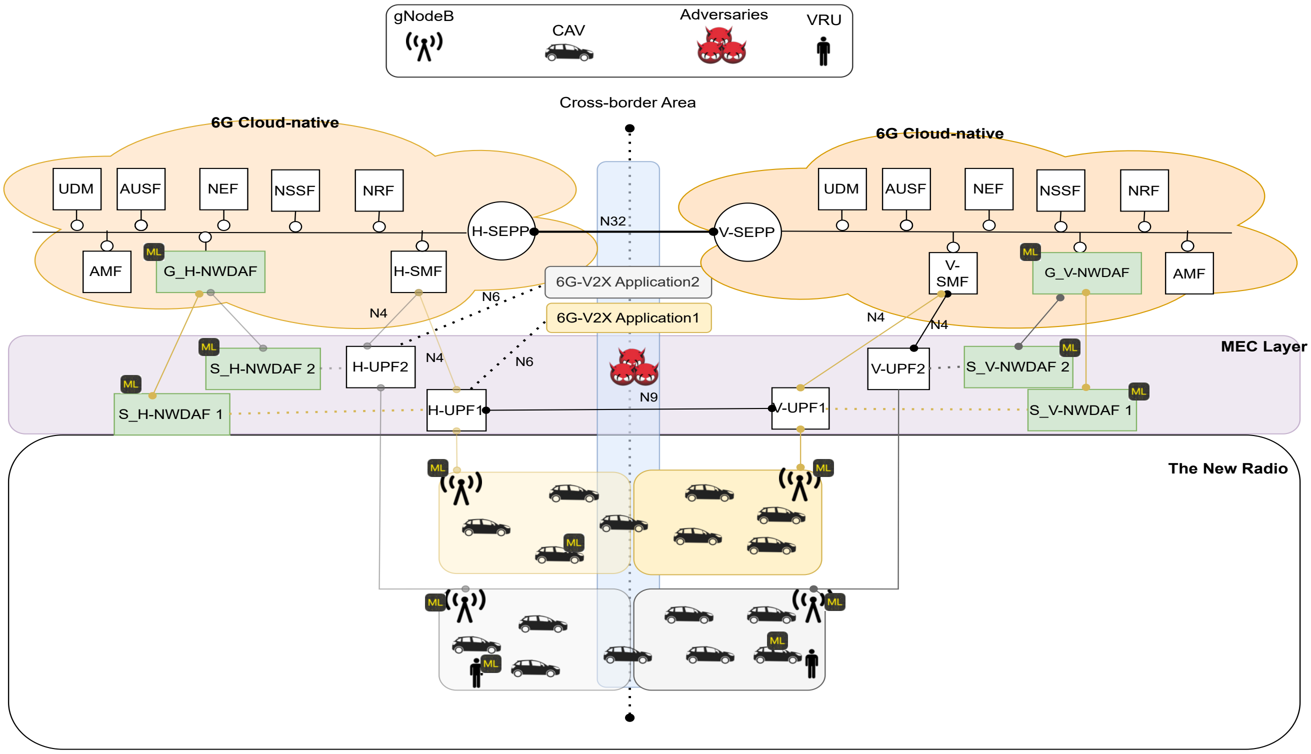

Fig. 1: 6G-V2X security for network slicing in cross-border scenario

Unified Data Management (UDM) | Authentication Server Function (AUSF) | Network Exposure Function(NEF) | Network Slice Selection Function (NSSF) | Network Repository Function (NRF) | Access and Mobility Management Function (AMF) | User Plane Function (UPF)

ever, the SEPP offers security only for the messages of the control plane. The data plane protection is provided by the Inter-PLMN User Plane Security (IPUPS) feature enabled in H-UPF and V-UPF, which H-SMF and V-SMF manage, respectively. IPUPS protects the GTP-U (GPRS Tunneling Protocol-User) data traffic by detecting and removing invalid traffic passing via the N9 interface and forwarding only valid data traffic [8].

4 Adversary model

While the current security standard provides security to some extent, security challenges are higher in 6G-V2X-NS at cross-borders. Specifically, due to the time-sensitive nature of 6G-V2X applications, H-MNO and V-MNO should execute low-latency roaming procedures to maintain the performance of such applications. This may leave security vulnerabilities attackers can exploit before, during, or after CAVs cross borders. Specifically, the roaming of CAVs in 6G-NS could be separated into two phases. The first phase is when CAVs approach or pass the cross borders and are attached to the V-MNO. The priority for the V-MNO in the phase is to ensure service continuity and road safety by quickly assigning CAVs to a 6G-V2X-NS with functionalities similar to one in H-MNO. In the second phase, the V-MNO optimizes its selection and considers other parameters, such as service quality and security.

Both phases are vulnerable to attacks. In the first phase, attacks can exploit the non-synchronization of security policies between H-MNO and V-MNO related to CAVs to launch attacks, such as disabled IPUP services for 6G-V2X-NSs. In the second phase, attacks can exploit misconfigurations and information gained from system infiltration, such as the maximum number of sessions supported by V-UPF and the activation of security controls to launch the attacks. To this end, our adversary model includes attacks targeting the data plane, such as attacks that aim to break V-UPF, H-UPF, and GTP-U data traffic passing through the N9 reference point (between H-UPF and V-UPF) [23], or GTP-C passing through the N4 reference point (between H-SMF and H-UPF) [24] or even the N6 reference point between 6G-V2X application and H-UPF [25].

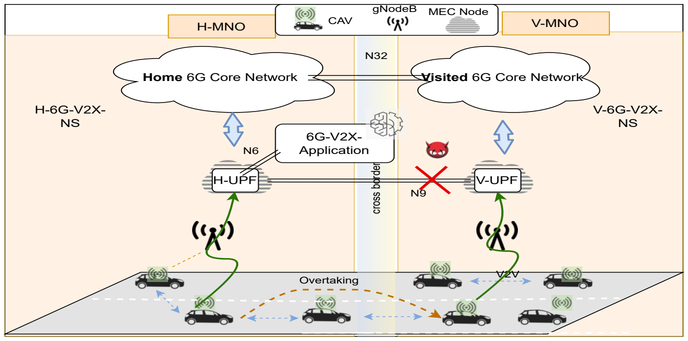

Fig. 2: Attacks on MEC-assisted automated highway-overtaking use case at a cross-border

These can critically impact 6G-V2X services such as MEC-assisted services and applications. A concrete example of such applications is related to the 5G-INSIGHT project[1]. Considering that the MEC-assisted automated highway-overtaking use case at a cross-border as illustrated in Figure 2. CAVs continuously send mobility-related to the MEC-based 6G-V2X application in this particular use case. The application processes the collected information and appropriately perceives the covered area. So, when a CAV requests maneuver permission with the required information attached, the MEC-based application processes the request and sends the authorization back to the CAV. Due to the mobility, this use case is attack-sensitive at the cross-border in the highway. For example, when a CAV attaches the V-MNO, it will route its messages to the MEC-based application through the link between V-UPF and H-UPF (reference point N9). So, if the attacker temporally breaks the link between H-UPF and V-UPF, the MEC-based application could be unaware or have a partial perception of the environment. Thus, the 6G-based V2X application can permit maneuver requests which may lead to dangerous road situations.

5 3GPP-COMPLIANT AND PRIVACY-PRESERVATION LEARNING 6G-V2X SECURITY AT CROSS BORDERS

Collaboration learning is required to protect 6G-V2X-NSs at cross-border against threats described in the previous section. Still, at the same time, networking and data privacy requirements should be respected. To address this, we propose a 3GPP-compliant scheme based on FL and stacking for security-related model training to detect 6G-V2X attacks at cross-borders. Specifically, this scheme uses multi-process federated learning to build multiple ML models for V2X network slices and then combines them to have a single global model for the MNO. More specifically, our scheme builds an ML model of every 6G-V2X-NS via an FL process. Every federated process runs for one V2X network slice with a dedicated FL server and includes FL clients only from that 6G-V2X-NS. Then, once all the ML models are ready, one of the models is selected, or all these models are combined using stacking to have a global model for the MNO. Moreover, this scheme builds ML models tailored for cross-border areas by combining models from the interconnecting MNOs. This section aims to describe the building blocks of our scheme. Specifically, we follow a top-button approach. We start by presenting the 3GPP-complaint security architecture for 6G-V2X NS. Then, we describe multi-process FL training for building security-related models and strategies to realize the global model of each MNO. After that, we describe how stacking is used to build a unified security-related model for accumulating attack-related knowledge of MNOs. Finally, we present the technical details of how FL and ensemble stacking are exploited in our scheme.

5.1 Hierarchical NWDAF architecture

Our approach exploits NWDAF and its services. NWDAF primarily aims at analytic reports to help other 5G Core network functions make optimal automated decisions. The latest 3GPP TS 23.288 specified that multiple instances of NWDAF may be deployed in a network [26]. We propose to build a hierarchical network of NWDAFs. Specifically, to maintain the isolation between 6G-V2X-NSs, we propose to dedicate an NWDAF, named *S-NWDAF*, for each 6G-V2X-NS. As shown in Figure 1, we propose to place *S-NWDAF* at the MEC layer close to the UPF to have a real-time update about network traffic and events. Moreover, we propose to extend *S-NWDAF* functionalities by adding three modules: 1) Learning module, which will be involved in training security-related ML models 2) Attack detection module, which takes charge of the detection of attacks within targeting the 6G-V2X-NS, and 3) Attack mitigation module, which automatically or in cooperation with the Security Operation System (SOC) thwarts the attack and applies mitigation mechanisms. While the second and third modules are part of our solution, this article mainly develops the learning module. This module enables FL processes within the 6G-V2X-NSs for training ML-related models.

Specifically, the learning module of each *S-NWDAF* acts as an FL server receiving model updates from FL clients selected from 6G-V2X-NS elements such as CAVs, VRU, gNodeB, and MEC nodes. After each round of the *S-NWDAF* aggregates the update parameters of the local models are to obtain the global model of each 6G-V2X-NS. Within the same MNO, all *S-NWDAFs* are connected to a global NWDAF, denoted *G-NWDAF*. This function is to deploy in the 6G core network (connected to all core functions via the (Service-Based Architecture (SBA) interface) and is discovered by NRF. The interactions between *G-NWDAF* and *S-NWDAFs* follow a producer-consumer model. Specifically, *G-NWDAF* subscribes to services provided by *S-NWDAF* as a Network Function (NF) consumer. More specifically, *G-NWDAF* is subscribed to $Nnwdaf\_MLModelProvision$ service, enabling it to receive a notification when the slice global model becomes available, and $Nnwdaf\_MLModelInfo$ service enables the *G-NWDAF* to request and get the global slice model [8].

5.2 Multi-process Federated and Realizing MNO's global model

Our approach proposes a multi-process FL architecture for 6G-V2X network slicing. Specifically, each FL process runs within each 6G-V2X-NS isolated from other FL processes. This section describes the FL multi-processes executed in each 6G-V2X-NS on both H-MNO and V-MNO. As shown in Algorithm 1, the procedure starts when *G-NWDAF* sends security parameters to every *S-NWDAF*$_i$. Security parameters consist of the initial parameters of the global models (old model parameters if applicable), and the number of FL rounds R to execute. Then, the *G-NWDAF* subscribes to $Nnwdaf\_MLModelProvision$ and $Nnwdaf\_MLModelInfo$ services of every *S-NWDAF*$_i$ to receive a notification when the global model M_i is ready and to get it respectively. Once a *S-NWDAF*$_i$ receives initial parameters, it can start the FL training process. At each round, the current global model M_i parameters are sent to a set D_i of selected data owners (FL client). A data owner d_j could be any V2X node in the NR, such as CAV, VRU,

[1] https://5g-insight.eu/

Algorithm 1: Cooperative model training

```
G-NWDAF sends initial model parameters $\omega$ and
  maximum rounds $R$ to every S-NWDAF ;
G-NWDAF subscribes to
  $Nnwdaf\_MLModelProvision$ and
  $Nnwdaf\_MLModelInfo$ services every
  S-NWDAF$_i$ ;
for each S-NWDAF$_i$ do
    for r=1 to to $R$ do
        for each data owner $d_j \in D_i$ do
            if ($d_j$ subscribed to 6G-V2X-NS$_i$ and selected
              by S-NWDAF$_i$) then
                Conduct local training on dataset $ds_j$
                  as described in subsection 5.4.1;
                Send parameters of local model $\omega_j(t)$
                  to S-NWDAF$_i$ through a secure data
                  plane channel;
            end
        end
        Aggregate the parameters in S-NWDAF$_i$ as
          described in subsection 5.4.2;
        Send back the parameters to $d_j \in D$ ;
    end
end
if $M_i$ is ready then
    G-NWDAF receives a notification from
      $Nnwdaf\_MLModelProvision$ that the model
      is ready ;
end
if G-NWDAF receives notification from all S-NWDAFs
  then
    G-NWDAF then requests from every S-NWDAF$_i$
      its $M_i$'s parameters;
end
if all models are received by G-NWDAF then
    G-NWDAF applies one of the two strategies:
        • Strategy 1 is to select the best-performing model.;
        • Strategy 2 performs stacking as described in
          Section 5.5;
end
```

gNodeB, and MEC node. Every round d_j receives the parameters of the global model M_i, trains its local model based on its local dataset ds_j, and sends back the parameters of its local model to *S-NWDAF$_i$*. The communication between *S-NWDAF$_i$* and data owner/FL-clients passed through the control plane and is encrypted and secured using TLS. Once the slice global model M_i is ready in *S-NWDAF$_i$*, the $Nnwdaf\_MLModelProvision$ service sends a notification to *G-NWDAF* to inform it that the model is ready. Once the *G-NWDAF* gets all notifications, it requests for models from $Nnwdaf\_MLModelInfo$ services. Once *G-NWDAF* receives all global models of 6G-V2X-NS, two strategies can be used. The first strategy is to select the best-performing model among the global models M= $\{M_1, M_2,..., M_i\}$. The selection can be automated using a validation data set provided by the SOC. In this case, all the models in M are tested on the validation data set. The model M_{i*} with the best accuracy is selected as a national global model to deploy as attack detection. This selection could also be made manually by the SOC. The second strategy is to perform the stacking among the set of models M as described in Section 5.5.

5.3 Differential privacy-enabled of building a unified global model

This section presented the proposed differential privacy-enabled stacking protocol. We first present some preliminary information on differential privacy. Then, we present the protocol steps.

5.3.1 Preliminaries on Differential privacy

Assume that M_i and M_j are two models. M_i is trained on D_i and M_j is trained on D_j for two nearby datasets D_i and D_j that differ only in one data point x. Let S represent the output space so that for an input of x, $M_i(x)$ and $M_j(x)$ are included inside S. Differential privacy (DP) ensures that an observer (adversary) cannot tell if a randomized mechanism $\mathcal{N}(M_i(x))$ or $\mathcal{N}(M_j(x))$ was based on D_i or D_j, i.e., whether or not x was used as a training example for $M_i(x))$ or $M_j(x)$, respectively [27]. The non-identifiability of x is safeguarded by the membership of x in D_i or D_j being indistinguishable. In (ϵ − δ)-DP, ϵ (also known as the privacy budget) parameterizes the indistinguishability of the outputs of $M_i(x)$ and $M_j(x)$, and δ denotes the failure probability of the mechanism $\mathcal{N}$. Lower $epsilon$ values signify more robust privacy protection. (ϵ − δ)-DP is formalized in Equation 1, when δ = 0, $\mathcal{N}$ is ϵ-DP.

$$P\left[\mathcal{N}(M_i(x)) \in S\right] \leq e^{\epsilon} * P\left[\mathcal{N}(M_j(x)) \in S\right] + \delta \qquad (1)$$

To guarantee ($\epsilon - \delta$)-DP, we apply a gradient perturbation technique with Differentially Private Stochastic Gradient Descent (DP-SGD) [28]. The algorithm aims to limit the privacy loss per gradient update by post-processing the gradient update in 2 steps:

- Clipping the gradients. In other words, scaling the gradients to have a C maximum L2 norm.
- Adding noise to the gradient updates proportionally to our clipping norm C. The noise is taken as a sample from a Gaussian with a (C * σ) standard deviation. σ is the so-called noise multiplier.

$$\theta_{t+1} = \theta_t - \eta_t \tilde{g}_t \qquad (2)$$

Equation 2 gives how DP-SGD updates the gradients at each training step. η_t is the learning rate and $\tilde{g}_t$ is the clipped gradient after adding noise. The hyperparameters C and σ can be adjusted to provide a certain ($\epsilon - \delta$) guarantee at each training phase.

5.3.2 Differential privacy-enabled stacking

Once each MNO finishes building its security-related ML model, the MNOs exchange the parameters of their models via the secured N32 interface. This will help MNO collaborate by accumulating knowledge residing in ML models by applying the stacking method. However, sharing the MNO's

ML model can make it vulnerable to inference attacks and violate privacy preservation. To overcome this issue, we propose a differential privacy-enabled stacking protocol. Specifically, the MNOs first agree on a dataset used for stacking. This dataset is shared N32 interface and periodically maintained. Each NWDAF runs a stacking ensemble algorithm to build a unified global model, described in Section 5.5, with a few modifications. More specifically,

1) Each G-NWDAF (H/V) applies differential privacy to inject noise into its global model.
2) Each G-NWDAF (H/V) uses the global model of the local MNO (H/V) with the DP-enabled model of the other MNO (V/H) to execute the first stage of the stacking algorithm.
3) Each G-NWDAF (H/V) executes the second phase of the stacking algorithm as described in Section 5.5.

5.4 Federated Learning

FL is a distributed ML technique to reduce privacy issues, enabling several parties to train a global model collaboratively without revealing individual data sets [29]. Several FL clients work with the FL server to train a global ML model in the FL architecture[30]. The FL server trains the global model throughout several rounds until it produces a good global model. The FL server chooses a group of FL clients for each round and transmits either the original model or a model acquired after the previous round. Several criteria can contribute to the selection of FL clients [31]. Each FL client calculates its local updates of the global model using Stochastic Gradient Descent (SGD) based on the received model using its locally labeled data set. All of the chosen FL clients communicate their local updates to the FL server following the conclusion of the round. The FL server employs the Federated averaging (FedAvg) method to combine local updates to calculate the parameters of the global model. This section gives technical details on both local training and global averaging stages.

5.4.1 Local training

The local update of the model is computed using an objective function given in Equation 3, which aims at minimizing a loss function $L_k(\omega)$ of an FL client (k) with respect to ω. $L_k(\omega)$ can be calculated (across n_k data points). f_i (x_i,y_i;ω) is the loss of the prediction on the data point (x_i,y_i) made with model parameters ω.

$$\min_{\omega \in R^d} \frac{1}{n_k} \sum_{i \in D_k} f(x_i, y_i; \omega) \tag{3}$$

As we can see in Algorithm 2 (step 4), n_k data points are split into B sized batches by an FL client (k). In steps (5-9), k locally trains the received global model on E epochs. Specifically, k updates a local vector of weights $\omega \in R^d$ over B in each epoch e. Then, in step 10, k updates the global weight vector, where η is the learning rate, and Δ ℓ (ω; b) is the gradient of the local objective function of k.

Algorithm 2: Local training (k, ω)

```
1  Input: $n_k$
2  Output: $\omega^k$
3  Extract $n_k$ feature set ($x_i$,$y_i$)
4  $b$ ← Split data $n_k$ into batches of size $B$
5  for each local epoch e from 1 to $E$ do
6      for $b \in B$ do
7          $\omega^k \leftarrow \omega^k$ - $\eta$ $\Delta$ $\ell$ ($\omega$;$b$)
8      end
9  end
10 return $\omega^k$ to server
```

Algorithm 3: Global Averaging (r)

```
1  Input: $\omega_0$
2  Output: $\omega$
3  Initialize $\omega_0$
4  for each round r =1,2,... do
5      K ← desired number of FL clients
6      for each client $k \in K$ do
7          $\omega_{r+1}^k \leftarrow$ Local training($k$, $\omega$)
8      end
9      $\omega_{r+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} \omega_{r+1}^k$
10     $\omega \leftarrow \omega_{r+1}$
11 end
```

5.4.2 Global Averaging

The FL server uses the objective function given by Equation 4 to aggregate the global model.

$$\min_{\omega \in R^d} l(\omega) = \frac{1}{n} \sum_{i=1}^{n} f_i(\omega) \tag{4}$$

where,

$$l(\omega) = \sum_{i=1}^{K} \frac{n_k}{n} L_k(\omega) \tag{5}$$

As n_k might differ among the K clients, Equation 5 provides a weighted average from all the K FL clients. As shown in Algorithm 3 (Step 3), the FL server initializes global model weights. Then, in step 7, Local training(k, ω) updates ω_{r+1}^k for each client $k \in K$ for each r round. Finally, the weighted average of the aggregated client updates is calculated using the federated averaging method at each round r using Equation 6.

$$\omega_{r+1} = \sum_{k=1}^{K} \frac{n_k}{n} \omega_{r+1}^k \tag{6}$$

ω_{r+1} is the global weight at round $r+1$ for a total of K FL clients over a total of n data points.

5.5 Stacked generalization

Stacked generalization is one of the ensemble methods. It aims to train a new meta-learner model that combines the predictions from multiple existing sub-models to deliver better output predictions [32]. Specifically, the stacking procedure in Algorithm 4 takes sub-models as input and the stacking meta-learner as output. This procedure has two stages.

- **Stage 1 (lines 1-3)**: takes a set of sub-models EM= $\{M_1, M_2,..., M_s\}$ and makes the predictions based on the training dataset S for generating a new dataset S'.
- **Stage 2 (line 4)**: takes the output of level 1 (S') as an input to train a meta-learner M' for making better predictions.

Algorithm 4: Stacking

```
1 Input: Training data $S = \{x_i, y_i\}_{i=1}^{m}$, $EM$= $\{M_1,$
    $M_2,..., M_s\}$
2 Output: The stacking model $M$
3 for i=1 to to $m$ do
4     Construct a new data set $S'$ that contains $x'_i, y_i$,
       where $x'_i$ = $M_1(x_i)$,$M_2(x_i)$, ...., $M_s(x_i)$ ;
5 end
6 Train on a meta-learner $M'$ based on $S'$;
```

In our scheme, the stacking ensemble is used in two stages. The first one is when the MNO selects the second strategy to build its global model. In this case, the 6G-V2X-NS security-related models serve as sub-models for that stacking algorithm to build a meta-learner instead of choosing the best-performing model between the slice models of the same MNO. The second stage is building a unified model between the two MNOs, as Section 5.3.2 describes.

6 Performance Evaluation

This section evaluates the performance of our scheme. This section is divided into two subsections. We first describe our experiment settings. Then, we discuss the obtained results.

6.1 Experiment settings

To evaluate the scheme's performance, we have used the 5G-NIDD dataset [33], a recent dataset and one of the most realistic publicly available 5G datasets. This dataset was generated based on a 5G testbed connected to the 5G test network at the University of Oulu. For our experiments, we have used the combined version of 5G-NIDD available in IEEEDataPort, which includes data for all attack scenarios [34]. The used dataset contains $1,215,890$ instances (rows).

Table 3 lists the rows' distribution per each attack type. The dataset originally included 50 features with two labels. However, after performing feature selection, the number of features becomes 48 with only one label. Specifically, we removed the ”Attack_tool” feature and selected ”Attack_type” as a label for the training processes. In addition, we normalized dataset features to values in the range of [0,1] using the MinMaxScaler.

Furthermore, we have divided the dataset into three sub-datasets (i) the first sub-dataset is used in the multi-process FL architecture experimented for the H-MNO, (ii) the second sub-dataset is used in the multi-process FL architecture experimented for the V-MNO, and (iii) the third sub-dataset is used in the stacking process of H-MNO and V-MNO security-related models.

TABLE 3: Dataset distribution per attack

Attack type	Support
Benign	477737
UDPFlood	457340
HTTPFlood	140812
SlowrateDoS	73124
TCPConnectScan	20052
SYNScan	20043
UDPScan	15906
SYNFlood	9721
ICMPFlood	1155

In our settings, we assumed that each MNO managed three 6G-V2X-NSs. For each 6G-V2X-NS, we assumed five FL clients. In addition, we adopted two strategies to distribute data among the 6G-V2X-NSs of each MNO.

- In the first strategy, data is independently and identically distributed (IID) across 6G-V2X-NSs. In other words, attacks on 6G-V2X-NSs are independent and follow the same distributions across the 6G-V2X-NSs.
- In the second strategy, however, the distribution of attacks is different (non-IID). Specifically, 6G-V2X-NS 1, 2, and 3, respectively, include 80% of HTTPFlood attacks, 80% of SlowrateDoS attacks, and 80% of UDPFlood attacks. The remaining 20% of the previously mentioned attacks is equally shared between the other 6G-V2X-NSs. In addition, all the rest of the attacks are equally shared over 6G-V2X-NSs.

TABLE 4: Training parameters of the MNO's global model

Parameter	**Value**
Optimizer	SGD
Learning rate	0.01
Batch size	32
Dropout	0.75
Activation functions	ReLU, Softmax
The ratio of validation/test dataset	10%
# Rounds	100

The FL multi-processes for each MNO was implemented using Tensorflow and Keras Python libraries. Specifically, FL clients have been implemented as Tensorflow instances running local models. The global model was trained on the Google Colab platform. For the training process at each MNO, the dataset was split into training (80%), validation (10%), and test (10%) sub-datasets. The training and validation sub-datasets are used for the FL processes, while the test sub-dataset is used for stacking of 6G-V2X-NS security-related models. Besides, we adopted the same multi-class DL model for all FL processes, which consists of three layers: an input layer with 48 nodes, two hidden layers with 85 and 42 ReLU-activated nodes for each with a dropout of 0.75, and an output layer with 9 Softmax-activated nodes based on one hot encoding to recognize attacks. The weights of local models are calculated using SGD with a learning rate of 0.01 and mini-batches of size 32. After the end of each round, we use FedAvg to calculate the weight of the global model. The model's hyperparameters for FL processes are listed in Table 4.

For stacking, we have used a meta-learner consisting of (i) one input layer, where the number of nodes equals the number of stacked models, (ii) one hidden layer with 20 ReLU-activated nodes, and (iii) an output layer with 9 softmax-activated nodes. We have used ”ADAM” as an optimizer to train the stacking meta-learner for non-differential privacy-enabled settings. Moreover, to enable differential privacy, we use DP-SGD with the L2 norm clip equal to one, the noise multiplier equal to 0.9, the number of microbatches equal to one, and the learning rate equal to 0.01. The parameters of DP-SGD are listed in Table 5.

TABLE 5: The parameters of DP-SGD

Parameter	Value
Optimizer	DP-SGD
Learning rate	0.01
L2_norm_clip	1
Noise_multiplier	0.9
Num_microbatches	1

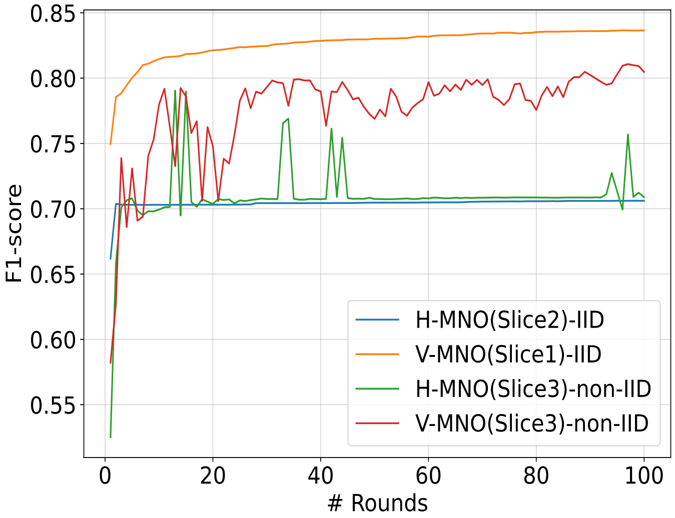

Fig. 4: The training accuracy of the best-performing security-related models of 6G-V2X-NSs for H-MNO and V-MNO on IID and non-IID.

6.2 Results

This subsection discusses our obtained results. It is divided into two parts. In the first part, we present the results obtained in training security-related models without using differential privacy. Then, in the second part, we study the impact of differential privacy on the accuracy of security-related models. We use the F1-score as a metric for our evaluations since we have conducted our experiments on an imbalanced dataset.

6.2.1 *Training results*

Figure 4 shows the training F1-score of the best-performing 6G-V2X-NS security-related models for each MNO on IID and non-IID configurations. Specifically, for the H-MNO, we found that the best security-related models are in 6G-V2X-NS 2 in the case of IID and 6G-V2X-NS 3 in the case of non-IID. On the other hand, for the V-MNO, the best-performing models were found in 6G-V2X-NS 1 and 6G-V2X-NS 3 for IID and non-IID, respectively. In addition, we can see that the V-MNO 6G-V2X-NS models outperform the H-MNO 6G-V2X-NS models on the validation dataset. This is mainly due to the quality of data that each MNO has. Moreover, we can see that the security-related models of 6G-V2X-NSs trained on the IID data perform better than those trained on non-IID data.

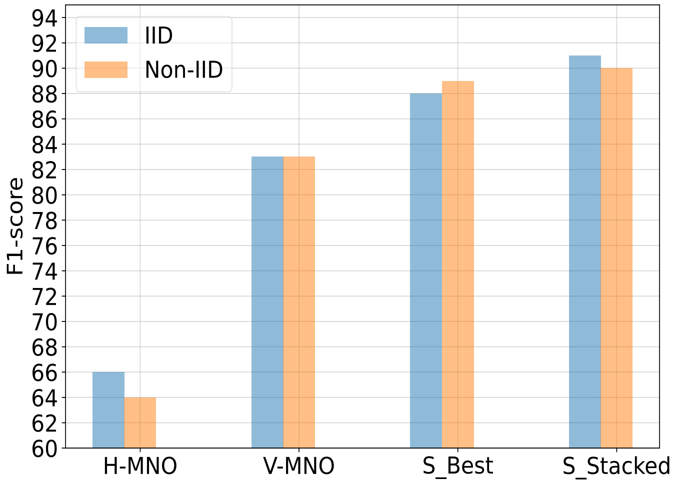

Fig. 5: Accuracy detection rates in the presence of poisoning attacks

In Figure 3, for each MNO, we compare the F1-score of security-related models of 6G-V2X-NSs with the F1-score of the MNO stacked model. The results show the F1-score of these security-related models on the test dataset. Specifically, Figure 3 (a) compares security-related models with the stacked model for the H-MNO. As we can see in this Figure, for the IID case, the security-related model of 6G-V2X-NS 2 outperforms all other security-related models and even the stacked model of H-MNO. On the other hand, for the non-IID case, we can see that the security-related model of 6G-V2X-NS 3 outperforms all other 6G-V2X-NS security-related models and the stacked model. Figure 3 (b) compares the F1-score of security-related models with the F1-score of the stacked model for the V-MNO. We can see that for both IID and non-IID cases, the stacked model outperforms the 6G-V2X-NS security-related models. These results show that stacking 6G-V2X-NS security-related models does not enhance the F1-score at the H-MNO but improves the F1-score at the V-MNO. The reason for that is stacking models with poor F1-score can create noise in the stacked model, preventing it from enhancing the F1-score, which is the case at H-MNO. However, for the V-MNO, the F1-score of the security-related models is high enough to improve the stacked model's F1-score.

In Figure 5, we compare the stacked models of H-MNO and V-MNO with the global stacked model. We compare two strategies to produce the global stacked model. The first strategy (S_Best) consists in stacking the best 6G-V2X-NS security-related-model of the H-MNO with the best 6G-V2X-NS security-related-model of the V-MNO. More specifically,

1) In the case of IID, we stacked the security-related model of 6G-V2X-NS 2 of the H-MNO with the security-related model of 6G-V2X-NS 1 of the V-MNO.
2) In the case of non-IID, we stacked the security-related model 6G-V2X-NS 3 of the H-MNO with the security-related model of V-MNO 6G-V2X-NS 3.

In the second strategy, $S\_Stacked$, we stacked the stacked models of H-MNO and V-MNO. As a first observation, we see that the global models produced by the two strategies outperform the (inner) stacked models of the MNOs. In addition, we see that the global model produced using $S\_Stacked$ is better than the global models produced using S_Best. It is worth mentioning that the two models are tested on the same test dataset. Moreover, the stacked model of the global models trained on the IID dataset produces better results than the global model trained on the non-IID dataset. The detailed results of the experiments done in this part are listed in Table 6. These results demonstrate that stacking helps aggregate security-related knowledge of H-MNO and V-MNO, increasing attack detection accuracy. Moreover, the results also show that stacking the stacked models of MNOs is better than stacking the best security-related models to take advantage of all 6G-V2X-NSs instead of only one.

TABLE 6: Dataset distribution for muli-class classification

Data	Model	Precision	Recall	F1-score
IID	H-MNO	0.73	0.73	0.65
	V-MNO	0.85	0.87	0.84
	S_Best	0.91	0.90	0.88
	S_Stacked	**0.92**	**0.92**	**0.91**
non-IID	H-MNO (Stacked-M)	0.56	0.73	0.63
	V-MNO	0.82	0.86	0.83
	S_Best	0.88	0.88	0.86
	S_Stacked	**0.90**	**0.90**	**0.88**

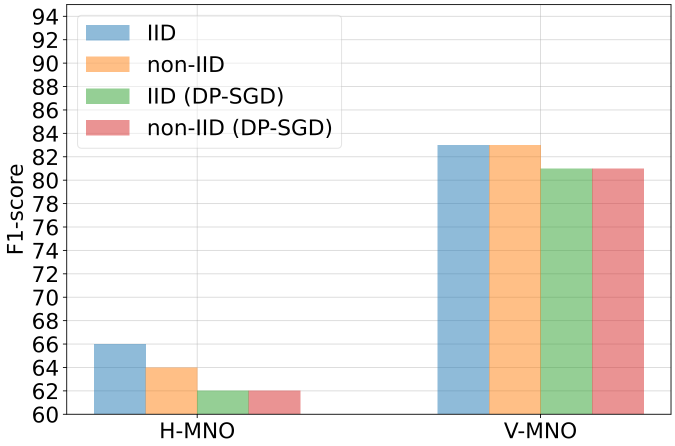

Fig. 6: The impact of differential privacy on the accuracy of H-MNO and V-MNO security-related models

6.2.2 *Impacts of Differential Privacy*

In this section, we evaluate the impact of differential privacy on the F1-score of security-related models. Specifically, Figure 6 compares the accuracy of security-related models of H-MNO and V-MNO without and with differential privacy by training it using DP-SGD on both IID and non-IDD cases. We can see, as expected, that using DP-SGD, the F1-score of security-related models for both H-MNO and V-MNO decreases a little bit due to the added noise for the sake of privacy guarantee.

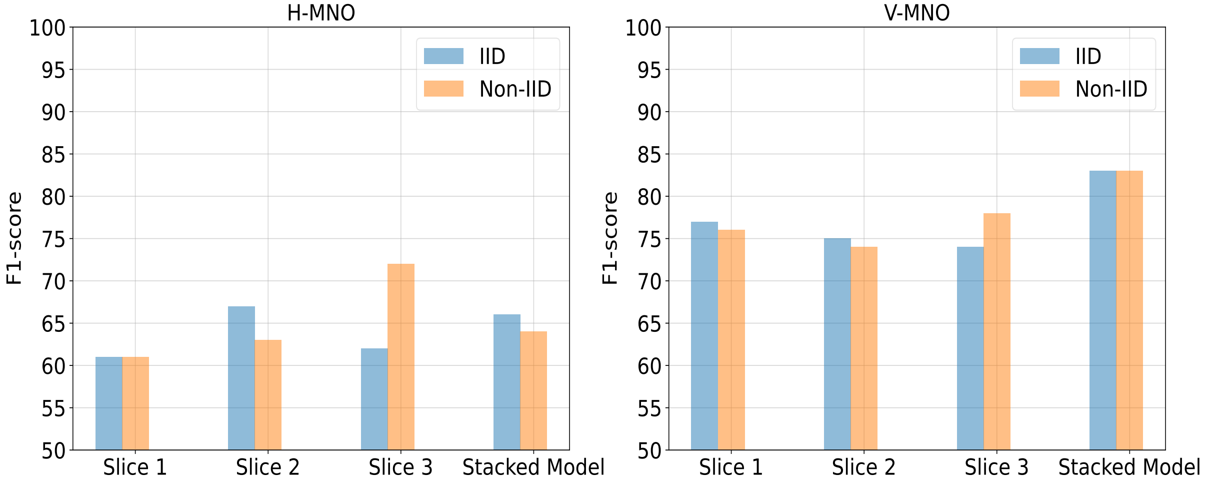

Fig. 3: Comparison the accuracy of security-related models of 6G-V2X-NSs with the accuracy of the stacked model for each MNO

Figure 7 compares the F1-score of global stacked in both H-MNO and V-MNO with and without differential privacy on IID and non-IID datasets. Specifically, S_Stacked_H-MNO (DP) stacked the H-MNO security-related model with the DP-enabled V-MNO security-related model. Similarly, S_Stacked_V-MNO (DP) stacked the DP-enabled security-related model of H-MNO with the security-related model of V-MNO. The results show that only S_Stacked_H-MNO (DP) is impacted by the applied differential privacy measure. Indeed, for both cases IID and non-IID the accuracy of S_Stacked_V-MNO (DP) equals to S_Stacked (without DP). The reason for this is that due to the low accuracy of the security-related model of H-MNO its impact on the stacked model is low compared to the security-related model of V-MNO.

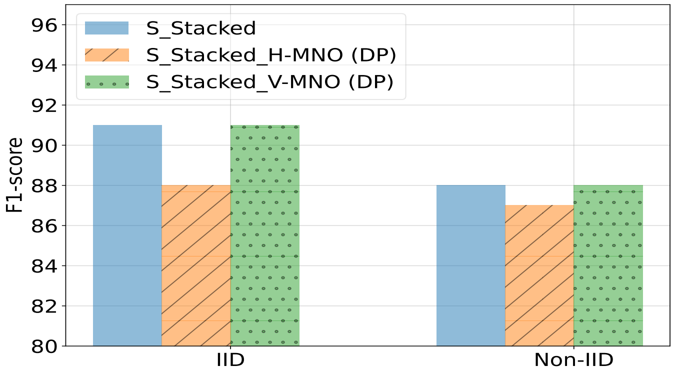

Fig. 7: The impact of differential privacy on the accuracy of the stacked global security-related model in H-MNO and V-MNO

The details of results presented in Figure 6 and Figure 7 are given in Table 7. In addition, table 7 shows the training time of the models. As we can see, using DP increases training time with the stacked models of MNOs, but it has no impact on stacking H-MNO and V-MNO global models.

TABLE 7: The impact of differential privacy

Data	Model	F1-score	training time (s)
IID (No-DP)	H-MNO	0.66	7.42
	V-MNO	0.83	6.13
	S_Stacked_H-MNO	0.91	16.77
	S_Stacked_V-MNO	0.91	15.58
IID (DP)	H-MNO	0.62	40.87
	V-MNO	0.81	36.85
	S_Stacked_H-MNO	0.88	15.76
	S_Stacked_V-MNO	**0.91**	15.58
Non-IID (No-DP)	H-MNO	0.64	2.37
	V-MNO	0.83	2.18
	S_Stacked_H-MNO	0.88	16.77
	S_Stacked_V-MNO	0.88	15.58
Non-IID (DP)	H-MNO	0.62	39.36
	V-MNO	0.81	42.72
	S_Stacked_H-MNO	0.87	14.39
	S_Stacked_V-MNO	**0.88**	15.01

In Figure 8, we conduct a privacy analysis to quantify the DP guarantee achieved in training security-related models. Specifically, we analyze privacy budget ϵ, which is a metric to evaluate an ML algorithm's DP guarantee as described in subsection 5.3.1. A smaller ϵ value indicates a better privacy guarantee. We perform an analytic evaluation by computing ϵ using compute_dp_sgd_privacy, a tool provided by Tensorflow Privacy, varying the noise multipliers. As we can see, increasing the noise multiplier will decrease the privacy budget and, thus, more privacy preservation. In our experiments, we set the noise multiplier to 0.9, which gives a good trade-off between privacy and accuracy.

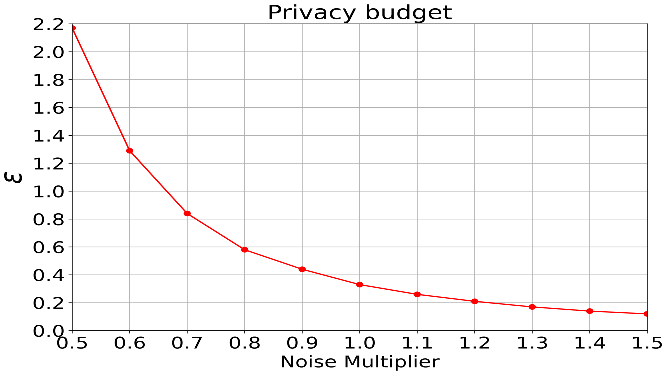

Fig. 8: Privacy budget analysis considering noise multiplier

7 Discussion

This section discusses the results obtained in our paper. The results demonstrate that muli-process FL with stacking can deliver high accuracy while ensuring isolation between 6G-V2X-NSs and privacy preservation between H-MNO and V-MNO. In addition, the results show that stacking is efficient for accumulating knowledge of security-related MNO models, especially when the accuracy of the models to be stacked is good. Moreover, the results show the impact of DP in stacking the global model is negligible when DP is applied to the security-related MNO's model with less accuracy. Furthermore, it is important to highlight that the solutions presented in this paper are also valid for multi-MNO scenarios involving several countries, such as the case of Luxembourg, France, Germany, and Belgium corridor. In this case, security-related models can be peer-to-peer stacked between MNOs or centrally stacked in a trusted server. Finally, our approach shows high flexibility since the security-related models of 6G-V2X-NSs can selectively be stacked between MNOs depending on the accuracy, context, attacks, or application. Besides, our scheme ensures the isolation of 6G-V2X network slices by design. Specifically, the FL processes are isolated from each other. Data, FL server, and FL clients are private for 6G-V2X each slice. Furthermore, it is worth mentioning that comparing our scheme's analytical results with related schemes will not bring meaningful conclusions. This is mainly because no related works have used the same dataset to demonstrate the performance of their scheme.

8 Conclusion

The failure to protect 6G-V2X network slices in cross-border scenarios may have catastrophic consequences. This paper employed federated learning and stacking for collaborative privacy learning between home and serving MNOs for securing 6G-V2X network slices. The results demonstrate collaboration between MNOs through our scheme is efficient in accumulating knowledge and better encountering attacks on 6G-V2X network slices while ensuring isolation between 6G-V2X network slices and privacy preservation. In future work, we further study multi-MNO scenarios in the case the global model is stacked in a common server and how to ensure the security and privacy of the server and MNOs. In addition, we plan to complement our scheme with attack detection and mitigation building blocks and establish the interactions between all these building blocks.

Acknowledgment

This work was supported by the 5G-INSIGHT bilateral project (ID: 14891397) / (ANR-20-CE25-0015-16), funded by the Luxembourg National Research Fund (FNR), and by the French National Research Agency (ANR).

References

[1] K. B. Letaief, Y. Shi, J. Lu, and J. Lu, "Edge artificial intelligence for 6g: Vision, enabling technologies, and applications," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 1, pp. 5–36, 2021.

[2] W. Wu, C. Zhou, M. Li, H. Wu, H. Zhou, N. Zhang, X. S. Shen, and W. Zhuang, "Ai-native network slicing for 6g networks," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 96–103, 2022.

[3] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6g: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[4] M. H. C. Garcia, A. Molina-Galan, M. Boban, J. Gozalvez, B. Coll-Perales, T. Şahin, and A. Kousaridas, "A Tutorial on 5G NR V2X Communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1972–2026, 2021.

[5] "Cyberattack Causes Trains to Stop in Denmark," https://www.securityweek.com/cyberattack-causes-trains-stop-denmark/, accessed: 2023-02-15.

[6] A. Kousaridas, M. Fallgren, E. Fischer, F. Moscatelli, R. Vilalta, M. Mühleisen, S. Barmpounakis, X. Vilajosana, S. Euler, B. Tossou *et al.*, "5g vehicle-to-everything services in cross-border environments: Standardization and challenges," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 22–30, 2021.

[7] A. Boualouache, B. Brik, Q. Tang, S. Cherrier, S.-M. Senouci, E. Pardo, R. Langar, T. Engel *et al.*, "5G Vehicle-to-Everything at the Cross-Borders: Security Challenges and Opportunities," *IEEE Internet of Things Magazine*, 2022.

[8] 3GPP TS 33.501, "Security architecture and procedures for 5G system (Release 17)," Sep 2022.

[9] N. Alliance, "5g security recommendations package," *White paper*, 2016.

[10] V. N. Sathi and C. S. R. Murthy, "Distributed slice mobility attack: A novel targeted attack against network slices of 5g networks," *IEEE Networking Letters*, vol. 3, no. 1, pp. 5–9, 2020.

[11] J. Wang and J. Liu, "Secure and reliable slicing in 5g and beyond vehicular networks," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 126–133, 2022.

[12] A. Boualouache and T. Engel, "A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2023.

[13] A. Thantharate, R. Paropkari, V. Walunj, C. Beard, and P. Kankariya, "Secure5g: A deep learning framework towards a secure network slicing in 5g and beyond," in *2020 10th annual computing and communication workshop and conference (CCWC)*. IEEE, 2020, pp. 0852–0857.

[14] N. A. E. Kuadey, G. T. Maale, T. Kwantwi, G. Sun, and G. Liu, "Deepsecure: Detection of distributed denial of service attacks on 5g network slicing—deep learning approach," *IEEE Wireless Communications Letters*, vol. 11, no. 3, pp. 488–492, 2021.

[15] B. Bousalem, V. F. Silva, R. Langar, and S. Cherrier, "Deep learning-based approach for ddos attacks detection and mitigation in 5g and beyond mobile networks," in *2022 IEEE 8th International Conference on Network Softwarization (NetSoft)*. IEEE, 2022, pp. 228–230.

[16] S. Wijethilaka and M. Liyanage, "A federated learning approach for improving security in network slicing," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022, pp. 915–920.

[17] R. F. Olimid and G. Nencioni, "5g network slicing: A security overview," *IEEE Access*, vol. 8, pp. 99 999–100 009, 2020.

[18] A. Boualouache, T. E. T. Djaidja, S.-M. Senouci, Y. Ghamri-Doudane, B. Brik, and T. Engel, "Deep learning-based intra-slice attack detection for 5g-v2x sliced networks," in *2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*. IEEE, 2022, pp. 1–5.

[19] A. Boualouache and T. Engel, "Federated learning-based inter-slice attack detection for 5g-v2x slicing networks," in *2022 IEEE 96th Vehicular Technology Conference:(VTC2022-Fall)*. IEEE, 2022, pp. 1–6.

[20] R. Keller, D. Castellanos, A. Sander, A. Robison, and A. Abtin, "Roaming in the 5g system: The 5gs roaming architecture," *Ericsson Technology Review*, vol. 2021, no. 6, pp. 2–11, 2021.

[21] ZTE Corporation, "Full-Scenario UPF Deployment White Papes," Dec 2020. [Online]. Available: https://res-www.zte.com.cn/mediares/zte/Files/newsolution/Wireless/CCN/hexinwang/whitepaper/ZTE_Full-Scenario_UPF_Deployment_White_Paper.pdf

[22] GSMA Association, "An Introduction to Network Slicing," 2017. [Online]. Available: https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf

[23] S. Park, S. Kwon, Y. Park, D. Kim, and I. You, "Session management for security systems in 5g standalone network," *IEEE Access*, vol. 10, pp. 73 421–73 436, 2022.

[24] G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, W. Mallouli, A. Cavalli, D. Klonidis, E. Markakis, and P. Sarigiannidis, "Threatening the 5g core via pfcp dos attacks: the case of blocking uav communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, pp. 1–27, 2022.

[25] S. Kukliński, K. Szczypiorski, K. Wrona, and J. Bieniasz, "5g-enabled defence-in-depth for multi-domain operations," in *MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*. IEEE, 2022, pp. 1024–1029.

[26] 3GPP TS 23.288, "Architecture enhancements for 5G System (5GS) to support network data analytics services," Sep 2022.

[27] I. Jarin and B. Eshete, "Pricure: privacy-preserving collaborative inference in a multi-party setting," in *Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics*, 2021, pp. 25–35.

[28] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.

[29] Z. Du, C. Wu, T. Yoshinaga, K.-L. A. Yau, Y. Ji, and J. Li, "Federated learning for vehicular internet of things: Recent advances and open issues," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 45–61, 2020.

[30] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečnỳ, S. Mazzocchi, H. B. McMahan *et al.*, "Towards federated learning at scale: System design," *arXiv preprint arXiv:1902.01046*, 2019.

[31] M. Chahoud, H. Sami, A. Mourad, S. Otoum, H. Otrok, J. Bentahar, and M. Guizani, "ON-DEMAND-FL: A Dynamic and Efficient Multi-Criteria Federated Learning Client Deployment Scheme," *arXiv preprint arXiv:2211.02906*, 2022.

[32] D. H. Wolpert, "Stacked generalization," *Neural networks*, vol. 5, no. 2, pp. 241–259, 1992.

[33] S. Samarakoon, Y. Siriwardhana, P. Porambage, M. Liyanage, S.-Y. Chang, J. Kim, J. Kim, and M. Ylianttila, "5g-nidd: A comprehensive network intrusion detection dataset generated over 5g wireless network," *arXiv preprint arXiv:2212.01298*, 2022.

[34] "5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network," https://ieee-dataport.org//documents//5g-nidd-comprehensive-network-intrusion-detection-dataset-generated-over- accessed: 2023-02-14.

Abdelwahab Boualouache is a research associate at the Faculty of Science, Technology and Medicine (FSTM), University of Luxembourg. He received a Ph.D. in computer science from USTHB University, Algeria, in 2016. His research interests include AI-driven security and privacy for 5G and Beyond Networks.

Amirhossein Adavoudi Jolfaei is currently pursuing his Ph.D. in the Department of Computer Science at the University of Luxembourg. He obtained his M.S. degree from the University of Isfahan in 2017. His primary research interests encompass privacy-preserving in vehicular networks, designing lightweight security protocols, secure computation, and security in wireless sensor networks (WSNs).

Thomas Engel is a Professor of Computer Networks at the University of Luxembourg. He received the title Dr. rer. nat from the University of Saarbruecken, Germany in 1996. Since 2002, he has taught and conducted research as a professor at the IST/University of Luxembourg. His SECAN-Lab team deals with performance, privacy, and identity handling in Next Generation Networks.