Federated Platooning: Insider Threats and Mitigations

Franco Callegati, Maurizio Gabbrielli, Saverio Giallorenzo, Andréa Melis, Marco Prandini

Federated Platooning: Insider Threats and Mitigations

Franco Callegati[†], Maurizio Gabbrielli[†,⋆], Saverio Giallorenzo[◇], Andrea Melis[†], Marco Prandini[†]
[†]Università di Bologna, [⋆]INRIA, [◇]University of Southern Denmark
{franco.callegati, maurizio.gabbrielli, a.melis, marco.prandini}@unibo.it, saverio@imada.sdu.dk

Abstract

Platoon formation is a freight organization system where a group of vehicles follows a predefined trajectory maintaining a desired spatial pattern. Benefits of platooning include fuel savings, reduction of carbon dioxide emissions, and efficient allocation of road capacity. While traditionally platooning has been an exclusive option limited to specific geographical areas managed by a single operator, recent technological developments and EU initiatives are directed at the creation of an international, federated market for platooning, i.e., a consortium of platoon operators that collaborate and coordinate their users to constitute freights covering international routes. In this paper, we look at federated platooning from an insiders' perspective. In our development, first we outline the basic elements of platooning and federation of platooning operators. Then, we provide a comprehensive analysis to identify the possible insiders (employees, users, operators, and federated members) and the threats they pose. Finally, we propose two layered, composable technical solutions to mitigate those threats: a*) a decentralized overlay network that regulates the interactions among the stakeholders, useful to mitigate issues linked to data safety and trustworthiness and* b*) a dynamic federation platform, needed to monitor and interrupt deviant behaviors of federated members.*

1. Introduction

Platoon formation has been the subject of design and analysis since seminal works on control law of the late 1960's [1], to high-profile studies, projects, and initiatives of the 1990's and 2000's [2, 3]. At the essence of automatic platoon formation there is formation control [4, 5], where a group of either manned or autonomous vehicles follows a predefined trajectory while maintaining a desired spatial pattern. With respect to conventional systems, the advantages of moving in formation include system optimization (like fuel saving, polluting emissions reduction, as well as efficient road usage [6]) and enhanced road safety, thanks to the respect of normed movements among vehicles (e.g., vehicle-to-vehicle distances, planned overtakes, etc.). The recent surge in mass-produced autonomous ground vehicles (both for the consumer and heavy-duty markets) has provided an additional stimulus to the development of advanced adaptive cruise control systems [7, 8]. This growing interest is also testified by the recent investments in the EU Roadmap for Truck Platooning[1] by the European Automobile Manufacturers Association, delineating the necessary steps to implement multi-brand platooning before 2025.

Indeed, while platooning is an effective solution suited in principle for nation-to-continent-wide applications, its most common implementations view platooning as a narrow-field option limited to specific categories (or brands) of vehicles, and confined to specific pertinence areas. These restrictions are mainly linked to the physical limitations of platooning operators, that are either allowed to operate within well-defined geographical boundaries, or require some specific infrastructural hardware for coordination (e.g., sensors, cameras, transmitters, etc.) of their services. Recently, new business models and support platforms have been proposed [9, 10, 11, 12] to share and market transport services owned by disparate transport operators. According to this new interpretation, transport operators can overcome previous limitations imposed by the topology of their pertinence areas through federations [13]. A federated operator can then buy transport services of other operators and offer these, along with its own, to its users, which perceive traveling as provided by a single operator. Adopting this view, also platooning can become a commodity where different operators, each with its own pertinence areas, can federate, collaborate, and coordinate their users to constitute freights covering international routes. However, while federation can maximize the benefits of platooning, its members increase their attack surface

[1] https://tinyurl.com/acea-platooning

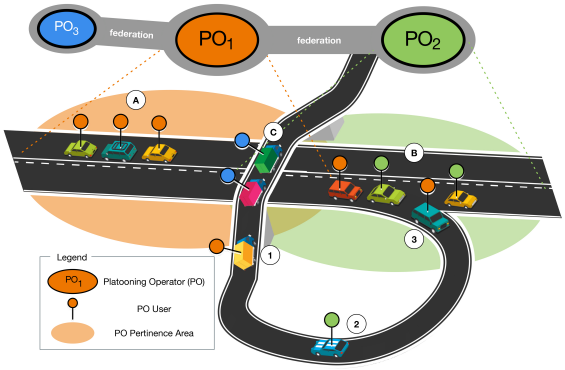

Figure 1. Examples of platoon formations in the federated scenario.

exposed to insiders within the federation. To understand this phenomenon and its implications over information systems and cyber-physical ones, this paper focuses on an analysis of the sensitive—yet elusive and frequently overlooked—issue of insider threats. In detail, in § 2 we introduce platooning and federation of platooning operators. Then in § 3 we identify the possible insiders and the threats they pose. Finally, we propose two composable solutions to mitigate the identified threats: *a*) a decentralized overlay network, described in § 4.1, that regulates the interactions among the stakeholders, useful to mitigate issues linked to data safety and trustworthiness and b) a centralized solution to monitor and interrupt deviant behaviors of federated members, presented in § 4.2, enabling the operation of a dynamic federation platform. To conclude, in § 5 we discuss related work from the general perspective of platooning and with respect to the proposed solutions and in § 6 we summarize results, limitations, and future developments of our work.

2. Federated Platooning

Here we describe the main concepts of traditional and federated platooning, as well as the elements needed to understand the security analysis presented in § 3.

To illustrate the main concepts and dynamics of platoon formation and federated platooning, we depict in Figure 1 a schematic representation of possible scenarios.

The most common reason found in literature to advocate platoon formation is to organize trucks that travel the same route in a row, so that the trail created by the first truck is used to reduce the fuel consumption of the trucks that follow the queue [14], but many other local or global efficiency parameters can be taken into account. For the sake of simplicity, in the examples that follow we abstract from the parameters (fuel consumption, polluting emissions, road capacity) that each platoon operator wants to optimize; we assume that platooning operators can reach a mediated agreement, and rather focus on describing their interactions in platoon formation. For starter, let us concentrate on the convoy pointed by label Ⓐ: it is an example of the simplest, traditional case of a platooning service, capturing the basic occurrence in the literature, in which users of the same platooning operator are coordinated by its central authority (PO_1).

The scenario pointed by label Ⓑ represents federated platooning: vehicles in the convoy are users of different operators (PO_1 and PO_2) and some of these (marked in orange) are outside the pertinence area of their operator. In this case, PO_1 and PO_2 coordinated the formation of a mixed convoy. In Ⓑ, PO_1 and PO_2 negotiated business policies for service usage to mediate possibly conflicting formation-control logics they deployed inside their networks. To better understand this concept, let us suppose that the two operators consider, in their respective platoon formation algorithms, the two constraints of cruise speed and fuel consumption. Although they account for the same parameters, PO_1 could offer to its users solutions that maximize cruise speed while PO_2 could favor fuel savings. However, thanks to agreed business policies in the federation, they may reach a distributed consensus over a mediated solution, satisfying the threshold parameters of their convoy formation algorithms. To draw a parallel, such a negotiation is similar to the one traditionally conducted among mobile phone operators to allow their users to roam within their networks.

Moreover, while traditional platoon formation relies on a static plan where vehicles join and leave a formation at predetermined times, the federation of platooning operators allows for a higher degree of flexibility: platooning users can decide to switch among different convoys participated by users of other operators. This last scenario is exemplified by the vehicle leaving the column in Ⓑ to join the convoy in Ⓒ. The column pointed by label Ⓒ, composed of the two users of operator PO_3, is outside the pertinence area of their home operator. Also in this case, although the column is composed only of vehicles of the same operator, the platooning plan results from a negotiation between operator PO_3, provider of the vehicles and PO_1 controller of the traveling area. Finally, thanks to the collaboration between all operators, the three vehicles ①, ②, and ③ can join the preformed convoy in Ⓒ.

In such a landscape, clearing functionalities must be made available to operators willing to collaborate.

Clearing is a founding concept in federated scenarios where self-interested parties share resources from different administrative domains [15]. The concept is drawn from finance, where "clearing of payments" denotes all the activities needed to turn a promise of payment into an actual movement of money from one account to another. In the context of platooning, clearing services are needed to correctly take into account the many factors that constitute costs for vehicle owners, and that need to be balanced with respect to the actual movements in a formation: for example, the first member of a platoon consumes more fuel than the rest of the convoy, vehicles joining/leaving platoons at different times undergo different cost schemes, etc. Moreover, since optimal platooning assumes its members to fulfill some pre-settled promises such as following planned routes and keeping intra-vehicle distances, one important factor for a reliable clearing system is risk management with respect to users reputation, e.g., their average degree of deviation from an agreed platooning plan. Clearing services are also useful to allow users to directly evaluate the actual gains (possibly expressed directly as monetary transactions) of many configurations, e.g., whether to join the tail of a formation or become the head of it, or switching between columns. This aspect holds also for users already in formation, which can agree to let other users join their formation and share the costs of the convoy. Beside direct user interaction, clearing costs and the related policies can be also part of the logic of composition among operators to select/propose optimal plans to their users. For example, with reference to the classical application to fuel savings, a federated platooning clearing system can be used in two distinct moments: *i*) prior to convoy formation, to calculate the effectiveness of joining positions according to different metrics such as the overall efficiency optimization or fairness maximization; *ii*) during convoy operation, to calculate how much each truck has gained or lost, in terms of fuel consumption by following others or opening the line, and to redistribute the profits on the basis of the actual routes and trips.

3. Threats and Mitigations

Once the main elements of platooning and federated platoon formation have been defined, it is possible to analyze the security concerns of such a global collaboration. These span from the illicit acquisition of sensitive data of users to the deployment of malicious platooning plans, which could result in a variety of consequences, ranging from inflicting economic losses to competitors, to affecting traffic over extensive areas, and even to threatening the safety of roads.

A federated environment natively foresees sharing one's own sensitive information, and access to others' information in a controlled way, for example to know basic data such as the kind of vehicles on the road, the most common routing choices, but in some cases also enough details to make tracking a vehicle or a driver possible. This kind of sharing is the core enabler for the desired aggregation services. Consequently, security concerns are greatly expanded as the attack surface is enlarged and diversified with respect to a closed-world model of operation. This kind of threats are not entirely specific of such platooning federated platforms; they would appear as an intrinsic aspect of any approach to coordinate services of independent transport agencies. Thus, they are interesting to address because results can be applied to a wider set of scenarios, and at the same time the analysis can be built upon previous works. For example, in [16] Callegati et al. show how the members of a public transportation consortium can exploit its clearing system to infer strategic private information.

In the remainder, we show how these kinds of attacks are relevant in a federated freight scenario: we describe the main issues introduced by platooning and evaluate their effects from an economic point of view, showing practical abuse cases, and highlighting the key vulnerabilities. In § 4 we present two, layered, composable technical solutions to mitigate the identified threats.

3.1. Concerns

The possible security problems of any platform based on controlled sharing of sensitive data are manifold and include threats such as: compromising the infrastructure where data is stored with the aim of subtracting it, intercepting data in transit by exploiting unsafe communication protocols, injecting falsified or malicious data by exploiting authentication weaknesses, and many others; these types of attack are not specific to our case study, but instead they are mainly related to the correct design and implementation of a data management infrastructure, a topic already widely covered in literature [17, 18, 19, 20], and for this reason they will not be discussed in this work.

Additionally, a complete threat analysis should include all the different agents operating against the system from the outside or within its boundaries, but the purpose of this work is to focus on the attacks that can come from an insider agent. The problem is not only the lack of proper countermeasures but also the difficulty of identifying a malicious insider in the first place [21].

Experts [22] agree that the strong contextual variance of threats makes providing a general yet precise

identification of all possible insiders difficult. Besides the members of the federation (here, the platooning operators), federated contexts contain two additional broad categories of insiders: *i*) legitimate users, which could leverage access to service providers and make a malicious use of information extracted from services or cause over-usages that entail unforeseen costs or outages; *ii*) orchestrating agents, which are needed to coordinate any complex architecture, can act as men-in-the-middle, accessing and/or leaking private information, as well as counterfeiting, throttling, hijacking or selecting data of legitimate users.

Hereinafter, we follow a categorization between privacy leakage attacks, where there is a theft of sensitive information, and disruption attacks, where an attacker interferes with the behavior or the structure of the system. We decided to focus only on these two categories of concerns for several reasons. First, we must remember that we are analyzing the concerns from an insider threat point of view. For this reason, we assume that we already have a certain level of permission within our infrastructure. This is why all targeted user attacks for initial access to the infrastructure are not particularly interesting. Second, we do not take into account attacks on the exploit of the infrastructure for lateral goals, since, although important, they are not the main cases of insider threat that can be found.

3.1.1. Privacy Leakage All the issues described in this section are a consequence of the kind of information that the clearing/platooning system needs to share and use. Examples of relevant categories of data and meta-data include:

- vehicle movements details: origin, destination, middle stops, average time, average speed, etc.
- details of shipped items: origin, destination, weight, package category, etc.
- route planning and execution constraints: clearing instructions applied to the current convoy, speed limits, etc.

While needed to enable operators' participation in platoon formation, the same information can be used by insiders together with external data sources to compose a targeted picture of sensitive aspects regarding a victim. The kinds of "retrievable" information are categorized in the following, based on the insider's target.

User Attacks A single user's privacy exploit is an attack that an insider can do in many ways. There are various effective methods to retrieve information about an individual driver even if it is not explicitly shared. If any database contains pseudo-identifiers, for example, the vehicle's serial number, they can be exploited to obtain the existing association between the vehicle id and the driver. For example, Callegati et al. in [23] demonstrated how to skim the various entries of a database, crossing them with external data from Open Source and publicly available OSINT tools and proceeding by exclusion to find the corresponding driver.

The process is described in principle in [24], where in a similar scenario of a data clearing system for urban public transport it was possible to trace a specific user's real identity by performing this kind of correlations. Knowing the precise movements and journeys of a vehicle driver is not only a powerful weapon against the vehicle driver's personal privacy; this information can be also used by competing companies to intercept the rivals' demand / supply patterns.

Business Policies Attacks For delivering companies, a fundamental competitive advantage derives from the methods and procedures with which they distribute the transport vehicles along their shipping routes. Indeed, it is shown [25, 26] that an efficient allocation of means of transport and drivers can reduce costs and management burdens. This information is strictly guarded by any company.

However, as explained above, to feed the necessary data into the clearing system, individual vehicle data must be (possibly partially) shared to calculate the correct redistribution of profits. In turn, illicit access or leakages of these data allow attackers to trace the distribution rules of the vehicles, as shown in [24], where through sequential analysis with clustering data mining algorithms the authors extracted the distribution of buses of a transport company present in a clearing system.

Unfair competition Lastly, we consider another type of sensitive information that an insider is able to retrieve. If information on vehicle routes and items carried is not properly anonymized, it is possible for insiders to cross them together and with external sources to interpolate financial details. Knowing which routes are the most profitable, what prices and which kinds of contracts companies offer on the same routes, makes it easy for unfair competitors to size contracts and deals [24].

3.1.2. Destructive Attacks The second category of attacks that an insider can launch goes beyond accessing an unauthorized resource and focuses on deriving advantages from the disruption of competitor's services.

An insider can try to achieve this result by injecting information in the clearing / platooning system. Carefully crafted malicious information may be the cause of a breakdown of competing services and businesses.

Routing corruption Let us consider a federated platooning system that holds all the data of the trucks and the shipped items of its members—as mentioned above, needed to calculate the correct redistribution of the profits and the management of platooning tasks. An insider might, in this case, inject malicious information aimed at excluding a specific route, causing denial-of-service targeted at one or more vehicle of a specific company. This exclusion can be achieved in several ways:

- declaring as additional meta-data fake speed limits to make the vehicle (think of time-guaranteed delivery trucks) late or to make a route plan inaccurately (in)convenient;
- posting false or incorrectly located traffic updates to force the competitor to change direction and redirect it to a wrong and / or inconvenient path;
- inserting non-existent routes that will force the vehicle to backtrack and recalculate along the way.

Competition starving The previous attack describes a targeted denial-of-service scenario, in which an insider attempts to block a competitor's specific service. The insider might wish, and be able, to do something more subtle. Instead of making a brutal intervention that causes a detectable disruption of a trip, the attacker could make a campaign of small, well-distributed manipulations that slowly impoverish the adversary economically. Such insertions, if successful, have the peculiarity that they cannot be immediately discovered, emerging only after a thorough and time-consuming analysis of the dataset. This kind of attack can be executed in several ways, for example:

- by performing the same kind of injections as described in the previous scenario, but introducing an error so small as to make it unlikely to be noticed as such, yet causing losses that end up having a disruptive cumulative effect;
- by making actual orders that force the competitor to deploy more vehicles (e.g., from a truck fleet) with lower profit margins, and possibly leveraging their presence to save more fuel from platooning.

4. Novel approaches to mitigation

The scientific literature provides various general techniques to mitigate the insider threats described in the previous section; these are summarized, as a reference, in § 6. In this section, we propose two layered technical solutions to tackle the data management issues outlined in the previous section. These two approaches stem from the observation that, from the point of view of data flow, it is not strictly necessary to have a centralized architecture to enable an effective exchange of information. On the other hand, information systems that support federation can be exploited to enforce correct behaviors of its members.

In the following, we first detail a decentralized overlay network for data safety and trustworthiness, then we describe the features of a dynamic federation platform, needed to monitor and interrupt deviant behaviors of federated members.

4.1. Overlay Network

A possible alternative to centralized data dispatching is to implement an overlay network created by the same entities of the federation. In this section we propose a solution based on a gossip protocol [27, 28], with the intent of mitigating the risk of sensitive information theft (eliminating the need of a centralized controller), and the risk of malicious data injection (implementing a trustworthiness source system that can guarantee the provenance of data).

Before describing the details of our proposed architecture, we provide a brief account on gossip-based networks, whose principles are at the basis of our overlay network. Gossip communication is a style of computer-to-computer communication protocol inspired by the form of gossip seen in social networks. Modern, large-scale distributed systems often use gossip protocols to solve problems that might be difficult to solve in other ways [29], e.g., because the underlying network either has an inconvenient structure or is extremely large. Computer systems typically implement this type of protocol with a form of random "peer selection": with a given frequency, each machine picks another machine at random and shares any hot rumors.

In our gossip protocol, users choose to gossip some information anonymously to a local administrators. Although anonymous, gossips are signed by a ranking grade owned by each user. In turn, local administrators aggregate (in a weighted manner) the gossips they received regarding the same objects (roads, point of interest, etc.) and re-gossip that information to users. By aggregating data (received within a certain time

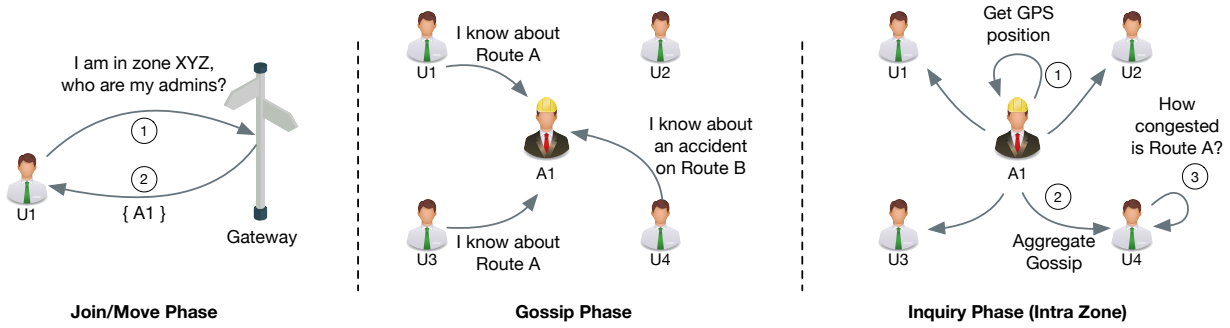

Figure 2. Phases of the Gossip Network.

span), administrators mitigate the diffusion of false information in the network, mediating (or ruling out) contrasting information. In our gossip protocol, nodes disseminate knowledge of their surroundings — e.g., a user is on a route and notifies the status of that road. Moving nodes periodically probe the network to join the partition to which they geographically belong, following a background dissemination approach. This recalls anti-entropy approaches that focus on providing a system-wide consistent observation as aggregate of many local responses. Thanks to the gossip protocol, we also anonymize the identity of users that query for information. In a traditional network, users would query a central server to retrieve some information, exposing their query (and themselves, by extension) to possible privacy attacks. On the contrary, in our setting it is the gossip protocol that is responsible for spreading information that might become relevant in the future to users. Hence we accept a trade-off of some overhead information to gain a privacy-by-design guarantee.

The concepts above are exemplified in Figure 2. From left to right, when users want to join for the first time or move between zones, they query known gateways to obtain the address of the administrator of the geographical region to which they currently belong. Administrators act as local zone authorities to route information about the same zone, and they can also provide (as gossip) their trustworthy data to users. In the gossip phase, users disseminate to administrators information regarding their surroundings. In Figure 2, U1 and U3 declare to know something about the route A congestion (e.g., rough road, slow traffic), while U4 has some information about a specific incident on Route B (e.g., closed roadways). The remaining phase regards the inquiry of available data. Users periodically receive aggregate (and possibly enriched) gossips from the local administrator and query the knowledge they acquired through gossiping to extract relevant information.

Figure 3 shows the two planes, over the physical one, that characterize the proposed overlay network. From the physical plane, users join the middle Neighborhood plane where they generate new gossip (in the Figure, the thicker the arrow, the more trustable the peer). On top, we find the Inquiry plane, where gossip spreads and where users inquiry their acquired knowledge.

A real world use case application for this overlay network can be a rough-road check. A service that exposes the real-time information about the road conditions is typically based on an algorithm that calculates an estimate, considering some previous information and the GPS position of the vehicle. This information is then saved on a centralized storage where the delay is calculated. As described above, however, this methodology introduces security problems on the storage of data and quality of service, entailed by relying exclusively on the users GPS location, which could possibly be inaccurate. With the proposed approach, we show how it is possible to improve the safety and performance of this type of service.

In Figure 3, U1 (Inquiry Plane) has been informed of the condition of the route it is currently following, so it could decide to perform a route deviation. This happened because it joined its local Neighborhood network, where other users (the blue and yellow cars that are further ahead on the route) have been gossiping ① (Neighborhood Plane) about its same route. In its turn, the administrator collected the gossips, aggregated them, and re-gossiped the information to the users ②.

Although users U2 and U3 remain anonymous, U1 can rate the quality of the aggregated information; a metric that can feed the system to assign the degree of trustability to users, as specified in the previous paragraph[2]. Besides security, the system enjoys a finer grade of precision on the reporting of the information as the machine-generated data from the administrator is integrated with user-generated, close-to-the-source information.

[2]Assignment of rankings to users can be spread back through gossip.

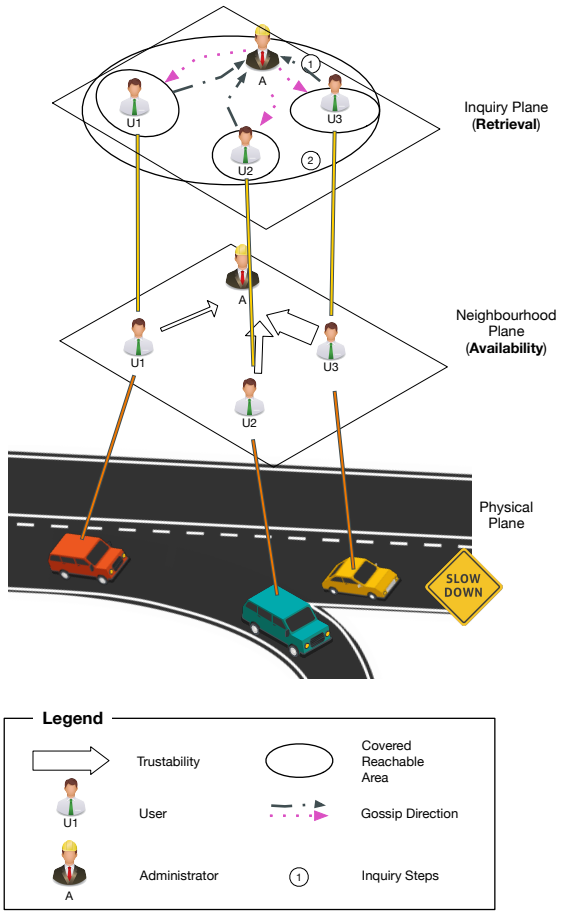

Figure 3. Depiction of the Overlay Gossip Network.

4.2. Automatic Business Policies and Contracts Enforcement

In § 3 we detailed how the platooning federation relies on the collaboration between operators, and how this gives the opportunity to malicious agents to adopt damaging behaviors. To prevent this, we want to introduce a mechanism to enforce the respect of the agreed behavior in the federation.

This is a common problem in all kinds of Service Oriented Architectures (SOA), as explicitly addressed in OASIS's SOA Reference Model [30]. According to OASIS definitions, policies define constraints for single services, and our approach is to let each provider and each consumer of services deal with data-related policies without forcing a centralization which could become the most valuable target for attacks. Contracts, on the other hand, "represent an agreement between two or more participants [...] a service contract is a measurable assertion that governs the requirements and expectations of two or more parties. Unlike policy enforcement, which is usually the responsibility of the policy owner, contract enforcement may involve resolving disputes between the parties to the contract. The resolution of such disputes may involve appeals to higher authorities. Like policies, contracts may be expressed in a form that permits automated interpretation."

Our proposal is to let that higher authority be represented by the platform enabling the federation. Rather than merely acting as an enabler, the information system supporting the federation shall connect each member based on the behavior that each operator declared and agreed to respect to join the federation. The support encompasses automated checking of contracts for compliance to general principles at design and deploy time, and the enforcement of contract provisions at run time. It is a part of a more comprehensive strategy for SOA management, as oulined in [31].

This shift moves federation from a static coalition of companies into a federated market, where operators dynamically partner with each other and trade and use services of one another on-demand, knowing that the agreed terms of usage will be respected. As remarked, this last guarantee is enforced by the platform itself, which will monitor the flow of requests and responses among the members, detect possible behaviors that deviate from the declared policy and limit or block the cooperation with an offending member.

In practice, contract specification is done when the platoon operator wants to join a federation. In this sense, enabling platforms shall provide respectively:

- a formal model with which to interpret policies and contracts;
- a set of specific requirements to satisfy in order to guarantee a safe environment;
- a set of policies regarding the use and the misuse of the services exposed;

In this context, business policies can have different purposes. For example, they can establish rules to mechanize the trading of the services of federated members, as well as to establish standards used in their interaction, like security and communication protocols, and define the terms of the quality of service. Automated policy processing allows automated contract design, to enable dynamic participation to the federation activities. In turn, contract enforcement at run time ensures all parties that everyone is held accountable against the designed contracts.

Beside security, we underline how these business policies are particularly important in the context of platooning operators, where each of them controls a specific, restricted area, while the platooning plan of a convoy

usually spans areas controlled by many operators. With automatized business policies platooning operators can collaborate in synthesizing a common platooning plan, possibly comprising a mixed set of their users.

A prototypical example of one such platform is [32], where the authors employ machine-processable business policies to federate remote instances in a federated platform and where transport operators that agree to the same (or better, to compatible) business policies can partner with each other and trade each other's transport services.

5. Related Work

To the best of our knowledge there are no works that consider and analyze insider threats in the context of federated platooning. However, there are some works close to ours, which consider security threats on traditional platooning, showcasing some vertical attacks. One example is the work of Dadras et al. [33] where they showed how through appropriate vehicle movements they were able to destabilize the vehicular platooning causing severe accidents. A similar attack analysis has been made in [34], where the authors went on to propose a safety-security co-design engineering process to derive functional security requirements.

Boeira et al. [35] proposed a study on a collaborative platooning approach. There, the authors evaluated several attack scenarios, similar to some of those we analyzed, identifying how platoons behave under varying attack conditions and what are the associated safety risks.

For what concerns the mitigations of such kind of attacks, literature abounds. The threats introduced by this federations of platform can be seen as an extensions of privacy and confidentiality issues of data management in XaaS platforms (Everything-as-a-service). For this reason, complementary to the two layered solutions proposed there are a set of data management solutions that, adapted to our specific context, can implement a secure, verifiable and safe platooning system.

To counteract pattern extraction attacks against privacy, it is possible to deploy sanitization techniques [36, 37, 38, 39]. These techniques must balance two needs: masking sensitive data versus keeping enough utility, i.e. information needed to perform the economic evaluations [40]. All the countermeasures for this kind of attacks are based on a trade-off between the amount of sensitive data preserved and utility of the queries.

Different anonymization and sanitization techniques have been proposed for complex datasets, but we need to introduce a measure that indicates the maximum amount of anonymized information such that the queries still work.

Different works proposed metrics for the evaluation of the amount of privacy preserved in specific dataset. A measure introduced in [41] defined an evaluation metric about the presence of pattern in a dataset called delta-presence. We can use this metric to evaluate the presence of a specific patterns in the shared dataset. Another interesting work in this direction is [36, 42] which operates by complementing existing techniques with post randomization methods.

Platforms for the automatic federation of members are suitable to integrate modules with functionalities like:

- sensitive data leakage prevention through masking of the raw datasets that reside in the centralized clearing system database;
- run-time, on line compliance checking of evolutive process changes by means of differential privacy protection evaluations;
- detection of privacy breaches by search of sensitive data on external data sources.

Injection of malicious data aimed at causing a denial-of-service is a difficult threat to mitigate. The main problem is that an injection prevention system must react on real-time to a specific attack, deciding if an event of data submission is legitimate or not.

Such Prevention Systems and more generally Intrusion Prevention Systems (IPS) work on the analysis of malicious models. The difference with our scenario is that a model can not be necessarily malicious (meaning as different from the regular ones). For this reason, the IPS of a clearing system should be applied to the analysis of the values, by detecting the range of suspects that will be eventually set under more in-depth analysis. Similar work has been done in real-time traffic control system [43] where data where buffered in specific amount and analyzed in such a way as to intercept a malicious value with a good trade-off between false positives and negatives. These attacks introduce real and legitimate values, but with a small error in real time that, spread on numerous injections, can lead to a considerable economic loss.

A longterm and deep analysis is required to detect these attacks, and once the attack is discovered, the attacker must be blocked. To do this it is therefore very useful to implement a rating mechanism for each individual user of the system. The inclusion of an error can be, in small quantities, completely legitimate. However, it is necessary to keep track of cumulated contributions and of the subsequent errors. For this reason a rating system that produces detailed feedback on the quality, quantity, and rating of data entered by

a particular user can block attackers in advance. An interesting rating mechanism has been described in [44] where the system classified feedbacks based on the user's role within the system, and by evaluating the quality of the data on a configurable set of options. Finally another interesting related work came from Laurendeau and Barbeau [45] where authors proposed a seminal work on the identification, ranking, and mitigations of security threats in WAVE, an architecture for vehicular networks used in platooning scenarios. Among the main threats from insider identified in [45] are denial of service/spamming attacks, data tampering, false data/malware injections, information eavesdropping, and identity masking/theft.

6. Conclusions

In this paper we investigated and proposed mitigations to insider threats concerning federated platooning, i.e., a freight organization system where a consortium of platooning operators collaborate and coordinate their users to constitute freights. From our threat analysis, we detailed novel technical solutions to the predominant threats of trustworthiness of data flows and deviant behaviors of federation members.

There are a few aspects that are worth a deeper investigation, mainly related to the practical implementation of the system; we thank the anonymous reviewers for helping us focus these limitations. Gossip protocols have been studied for more than a decade [46] and proved their effectiveness in many scenarios similar to ours, yet we need to quantify implementation costs and actual information dissemination robustness. Rating the trustworthiness of provided information is another aspect that received significant attention (see for example [47] and the cited related works). In our scenario, the positive results achieved by different means in other contexts could be hindered by the restricted number of members in each community; a detailed analysis is needed.

As future work, we plan to test and quantify the effectiveness of our solutions by simulating a series of prototypical platooning operators and conduct extensive tests, to assess the ability of the platform of identifying erroneous information and isolating misbehaving members, as well as to estimate the robustness of the platoon formation schemes to external disruptions.

References

[1] H. Y. Chiu, G. B. Stupp, and S. J. Brown, "Vehicle-follower control with variable-gains for short headway automated guideway transit systems," *Journal of Dynamic Systems, Measurement, and Control*, vol. 99, no. 3, pp. 183–189, 1977.

[2] S. E. Shladover, C. A. Desoer, J. K. Hedrick, M. Tomizuka, J. Walrand, W.-B. Zhang, D. H. McMahon, H. Peng, S. Sheikholeslam, and N. McKeown, "Automated vehicle control developments in the path program," *IEEE Transactions on vehicular technology*, vol. 40, no. 1, pp. 114–130, 1991.

[3] A. Geiger, M. Lauer, F. Moosmann, B. Ranft, H. Rapp, C. Stiller, and J. Ziegler, "Team annieway's entry to the 2011 grand cooperative driving challenge," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, pp. 1008–1017, Sept 2012.

[4] M. A. Lewis and K.-H. Tan, "High precision formation control of mobile robots using virtual structures," *Autonomous robots*, vol. 4, no. 4, pp. 387–403, 1997.

[5] J. A. Fax and R. M. Murray, "Information flow and cooperative control of vehicle formations," *IEEE transactions on automatic control*, vol. 49, no. 9, pp. 1465–1476, 2004.

[6] S. Tsugawa, "An overview on an automated truck platoon within the energy its project," *IFAC Proceedings Volumes*, vol. 46, no. 21, pp. 41–46, 2013.

[7] V. Milanés, S. E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, and M. Nakamura, "Cooperative adaptive cruise control in real traffic situations," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 296–305, 2014.

[8] K. Bengler, K. Dietmayer, B. Farber, M. Maurer, C. Stiller, and H. Winner, "Three decades of driver assistance systems: Review and future perspectives," *IEEE Intelligent Transportation Systems Magazine*, vol. 6, no. 4, pp. 6–22, 2014.

[9] S. Pippuri *et al.*, "Maas finland." http://maas.fi.

[10] F. Callegati, M. Gabbrielli, S. Giallorenzo, A. Melis, and M. Prandini, "Smart mobility for all - a global federated market for mobility-as-a-service operators," in *IEEE 20th International Conference on Intelligent Transportation Systems, ITSC 2017*, IEEE, 2017.

[11] V. Caiati, P. Jittrapirom, A.-M. Feneri, S. Ebrahimigharehbaghi, J. Narayan, and M. Alonso González, "Mobility as a service," *Urban Planning*, vol. 2, no. 2, 2017.

[12] C. Expósito-Izquierdo, A. Expósito-Márquez, and J. Brito-Santana, "Mobility as a service," *Smart Cities: Foundations, Principles, and Applications*, pp. 409–435, 2017.

[13] R. Buyya, R. Ranjan, and R. N. Calheiros, "Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services," in *International Conference on Algorithms and Architectures for Parallel Processing*, pp. 13–31, Springer, 2010.

[14] A. Lelouvier, J. Guanetti, and F. Borrelli, "Eco-platooning of autonomous electrical vehicles using distributed model predictive control," *parameters*, vol. 2, p. 4.

[15] A. AuYoung, B. Chun, A. Snoeren, and A. Vahdat, "Resource allocation in federated distributed computing infrastructures," in *Proceedings of the 1st Workshop on Operating System and Architectural Support for the On-demand IT InfraStructure*, vol. 9, 2004.

[16] F. Callegati *et al.*, "Insider threats in emerging mobility-as-a-service scenarios," in *HICSS*, AIS Electronic Library (AISeL), 2017.

[17] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, vol. 1, pp. 647–651, IEEE, 2012.

[18] S. Sakr, A. Liu, D. M. Batista, and M. Alomari, "A survey of large scale data management approaches in cloud environments," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 3, pp. 311–336, 2011.

[19] R. L. Krutz and R. D. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley Publishing, 2010.

[20] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1 – 11, 2011.

[21] S. Peisert, M. Bishop, L. Corriss, and S. J. Greenwald, "Quis custodiet ipsos custodes?: A new paradigm for analyzing security paradigms with appreciation to the roman poet juvenal," in *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, NSPW '09, (New York, NY, USA), pp. 71–84, ACM, 2009.

[22] A. Sarkar, S. Köhler, B. Ludäscher, and M. Bishop, "Insider attack identification and prevention in collection-oriented dataflow-based processes," *IEEE Systems Journal*, vol. 11, pp. 522–533, June 2017.

[23] F. Callegati, S. Giallorenzo, A. Melis, and M. Prandini, "Data security issues in maas-enabling platforms," in *Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), 2016 IEEE 2nd International Forum on*, pp. 1–5, IEEE, 2016.

[24] F. Callegati, A. Campi, A. Melis, M. Prandini, and B. Zevenbergen, "Privacy-preserving design of data processing systems in the public transport context," *Pacific Asia Journal of the Association for Information Systems*, vol. 7, no. 4, 2015.

[25] D. Gavalas, C. Konstantopoulos, and G. Pantziou, "Design and management of vehicle sharing systems: a survey of algorithmic approaches," *arXiv preprint arXiv:1510.01158*, 2015.

[26] J. Pfrommer, J. Warrington, G. Schildbach, and M. Morari, "Dynamic vehicle redistribution and online price incentives in shared mobility systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, pp. 1567–1578, Aug 2014.

[27] Z. J. Haas, J. Y. Halpern, and L. Li, "Gossip-based ad hoc routing," *IEEE/ACM Trans. Netw.*, vol. 14, pp. 479–491, June 2006.

[28] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Randomized gossip algorithms," *IEEE/ACM Trans. Netw.*, vol. 14, pp. 2508–2530, June 2006.

[29] M. Jelasity, A. Montresor, and O. Babaoglu, "Gossip-based aggregation in large dynamic networks," *ACM Trans. Comput. Syst.*, vol. 23, pp. 219–252, Aug. 2005.

[30] C. M. MacKenzie, K. Laskey, F. McCabe, P. F. Brown, and R. Metz, "Reference model for service oriented architecture 1.0," tech. rep., OASIS, 2006.

[31] T. Schepers, M. Iacob, and P. van Eck, *A lifecycle approach to SOA Governance*, pp. 1055–1061. ACM Press, 2008. Special track on Enterprise Information Systems.

[32] F. Callegati, M. Gabbrielli, S. Giallorenzo, A. Melis, and M. Prandini, "Smart mobility for all: A global federated market for mobility-as-a-service operators," in *20th International Conference on Intelligent Transportation*, 2017.

[33] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, pp. 167–178, ACM, 2015.

[34] J. Liu, D. Ma, A. Weimerskirch, and H. Zhu, "Secure and safe automated vehicle platooning," *IEEE Reliab. Mag.*, 2016.

[35] F. Boeira, M. P. Barcellos, E. P. de Freitas, A. Vinel, and M. Asplund, "Effects of colluding sybil nodes in message falsification attacks for vehicular platooning," in *Vehicular Networking Conference (VNC), 2017 IEEE*, pp. 53–60, IEEE, 2017.

[36] D. Molnar, B. Livshits, P. Godefroid, and P. Saxena, "Automatic context-sensitive sanitization," Nov. 25 2014. US Patent 8,898,776.

[37] R. Kissel, "Avoiding accidental data loss," *IT Professional*, vol. 15, pp. 12–15, Sept 2013.

[38] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–1, 2017.

[39] B. Ujwala and P. R. S. Reddy, "An effective mechanism for integrity of data sanitization process in the cloud," *European Journal of Advances in Engineering and Technology*, vol. 3, no. 8, pp. 82–84, 2016.

[40] M. Bishop, J. Cummins, S. Peisert, A. Singh, B. Bhumiratana, D. Agarwal, D. Frincke, and M. Hogarth, "Relationships and data sanitization: A study in scarlet," in *Proceedings of the 2010 New Security Paradigms Workshop*, pp. 151–164, ACM, 2010.

[41] M. E. Nergiz, M. Atzori, and C. Clifton, "Hiding the presence of individuals from shared databases," in *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, SIGMOD '07, (New York, NY, USA), pp. 665–676, ACM, 2007.

[42] B. R. Mistry and A. Desai, "Privacy preserving heuristic approach for association rule mining in distributed database," in *ICIIECS*, pp. 1–7, IEEE, 2015.

[43] S. Mirri, A. Melis, C. Prandi, and M. Prandini, "Crowdsensing for smart mobility through a service-oriented architecture," in *ISCC*, p. 5, IEEE, 2016.

[44] C. Prandi, P. Salomoni, and S. Mirri, "mpass: integrating people sensing and crowdsourcing to map urban accessibility," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, pp. 591–595, IEEE, 2014.

[45] C. Laurendeau and M. Barbeau, "Secure anonymous broadcasting in vehicular networks," in *32nd IEEE Conference on Local Computer Networks (LCN 2007)*, pp. 661–668, Oct 2007.

[46] M. Jelasity, A. Montresor, and O. Babaoglu, "Gossip-based aggregation in large dynamic networks," *ACM Trans. Comput. Syst.*, vol. 23, pp. 219–252, Aug. 2005.

[47] C. Prandi, S. Mirri, S. Ferretti, and P. Salomoni, "On the need of trustworthy sensing and crowdsourcing for urban accessibility in smart city," *ACM Trans. Internet Technol.*, vol. 18, pp. 4:1–4:21, Oct. 2017.