SOLVER: A Framework for the Integration of Online Social Networks with Vehicular Social Networks

Anna Vegni, Valeria Loscri, Abderrahim Benslimane

SOLVER: A Framework for the Integration of Online Social Networks with Vehicular Social Networks

Anna Maria Vegni*, Valeria Loscrí†, and Abderrahim Benslimane‡

*Department of Engineering, Roma Tre University, Rome, Italy. Email: annamaria.vegni@uniroma3.it (*corresponding author*)

†Inria Lille - Nord Europe, Lille, France. Email: valeria.loscri@inria.fr

‡CERI/LIA University of Avignon, Avignon, France. Email: abderrahim.benslimane@univ-avignon.fr

Abstract

Online Social Networks (OSNs) are comprised of people with social interactions and relationships, such as friendship and acquaintance. Social web communities (e.g., Facebook or Twitter), and content-sharing sites with social networking functionality (e.g., YouTube) have attracted millions of users, and OSNs are keeping on growing, with a giant number of users. At the same time, new social services are emerging, moving social networking from traditional OSNs towards Vehicular Social Networks (VSNs). VSNs consider a social network where every vehicle is capable of establishing social ties in an autonomous way with other vehicles or drivers/passengers. However, limitations in VSNs exist, like the reduced connectivity due to mobility models and the opportunistic nature of vehicular networks. Similar considerations apply in OSNs, where the centralized architecture may suffer of high traffic load. In this paper, the integration of OSNs with VSNs is realized through a hybrid framework that merges the centralized structure of OSNs with the distributed opportunistic nature of VSNs. The proposed hybrid OSN-VSN framework, namely SOLVER, allows communications both among different VSNs and towards OSN communities, in order to maintain connectivity and service alive that can be affected by mobility. Connectivity holes of VSNs can be limited through a handover procedure towards OSN community, as well as traffic load in OSN can be redirected to specific VSNs in order to release network resources in OSNs, with the consequent reduction of transmission delay. SOLVER presents a solution for maintaining connectivity in VSN and extending it towards OSN, and vice versa. Security and privacy

issues are also addressed through the use of a multi-layers security approach adopted in SOLVER. As a main strength, SOLVER is able to synergically exploits the positive features of OSNs and VSNs, as well as providing security and privacy, with mechanisms that are completely agnostic to the final users.

Index Terms

Vehicular Social Networks, Online Social Networks, framework, network architecture.

I. INTRODUCTION

Today, it is clearly a trend that the number of Online Social Networks (OSNs), like Facebook, Twitter, LinkedIn, etc., is increasingly growing [1]. OSNs present a centralized Client-Server (CS) network architecture that allows an always available service, accessible anytime and anywhere. Connectivity links among users of the same OSN community (a.k.a social ties) are always available, thus providing an always active and reliable online service.

Although social networking arises in OSNs, it applies also to other contexts, like vehicular scenarios where vehicles traveling on constrained paths (i.e., roads and highways) present a predictable social behavior due to their daily routine mobility patterns (i.e., spatio-temporal availability). From the definition of Internet of Vehicles (IoV) [2] that assumes an interconnected set of vehicles providing information for common services such as traffic management, road safety, and more in general infotainment, together with social networking features, Vehicular Social Networks (VSNs) [3] paradigm arises. Vehicular communications are then considered as the "first social network for automobiles," since each driver/vehicle can share data with other neighbors.

In a VSN, vehicles build their own social ties with other social objects they might come into contact i.e., neighboring vehicles and fixed road side units (RSUs), with the intent of creating an overlay social network to be exploited for information search and dissemination. VSN paradigm inserts in the middle of IoV and traditional OSNs, with specific features, such as (*i*) limited life time, (*ii*) limited access, and (*iii*) dynamic relationships [3]. Such features are mainly due to the opportunistic nature of VSNs. Connectivity links are not always available due to very dynamic speeds of nodes, as well as due to variable vehicular density in different environments. For such reasons, VSNs show a limited life time, as connections among nodes (i.e., social ties) can be lost due to the very dynamic vehicular scenario. On the other side, OSNs are built among

people with social relationships that are maintained stable anytime and anywhere (i.e., static ties). Also, OSNs typically are built on top of an infrastructure of servers, while VSNs are essentially a Peer-to-Peer (P2P) based architecture, due to the opportunistic nature of vehicular ad-hoc networking.

Security and privacy issues in VSNs lie on both the vehicle and driver/passenger, and attacks can affect the whole network very fast. Attackers can make use of the querying nature of P2P networks to overload the network, resulting in a broadcast storm that make the network inoperable. Furthermore, in VSNs, due to high variable connections, neighboring nodes can change very fast, thus providing anonymity among nodes, and affecting negatively security in VSNs.

Security and trust in VSNs are addressed through the Vehicular Public Key Infrastructure (VPKI) [4]. Each vehicle carries a Tamper-Proof Device that contains a unique and certified identity of the vehicle, and a set of certified anonymous public/private key pairs. Certificate exchange messages ensure that a safety message is from a trusted source. On the other side, in a CS network architecture like OSNs, a server is usually the target of massive connections, and attacks aim to render the server inoperable. Obviously, in OSNs security and trust mainly affect user profiles, requiring several solutions to guarantee acceptable security levels (i.e., authentication of users). Trust relationships among users have been explored to protect sensitive data or to verify the user's identity [5]. To summarize, Table I collects main differences existing between VSNs and OSNs [3].

This paper proposes a framework for the integration of OSNs with VSNs allowing to (*i*) overcome the well-known limitations of VSNs and (*ii*) extend the OSN structure to vehicular scenarios, resulting in a redirection of data flow to VSNs. The fixed and centralized network architecture of OSNs becomes a support to the decentralized and distributed VSNs with the aim of solving connectivity holes as typical of vehicular network scenarios. At the same time, VSNs can act as an extension of OSNs among members of VSNs, allowing a redirection of data flow towards mobile (vehicular) social networks.

Since VSNs reflect a typical P2P network architecture, they inherently rely on the dependence of peers to each other, and security implications arise from abusing the trust between peers. Authentication is more difficult to achieve in a pure P2P network architecture than in a centralized environment, because no central server is used to verify peers' identity. Authentication must be performed within the system between each pair or group of peers. Often, in pure P2P systems

TABLE I
FEATURES OF OSNS AND VSNS.

Feature	**OSNs**	**VSNs**
Architecture	Client-Server	Peer-to-Peer
Connectivity	Anytime, anywhere, always available	Spatio-temporal availability
Social ties	Strong and weak relationships	On-the-fly social ties
Social behavior	Static, where members are mostly the same with stable social ties	Dynamic, where members may change anytime based on interests and positions
Security	High level guaranteed by authentication mechanisms and more stable list of friends.	Low level due to dynamic connections and fast varying list of friends.

a third party (i.e., a central authority) is exploited in the authentication process, as well as it may be used to generate unique initial global identities for peers. In SOLVER, security and trust issues are addressed by different entities i.e., vehicles, RSUs, and Certificate Authorities (CA) that provide a security degree to drivers/passengers and vehicles themselves [6]. Specifically, driver/passenger's honesty factor is provided according to OSN-based trust by matching VSN and OSN user profiles. Vehicle's honesty is guaranteed through inter-vehicle interactions, while vehicle's location-related honesty computes a similarity measurement between the vehicle's current position and the estimated position, based on its historical mobility pattern.

The contributions of this paper are as follows:

1) We present the network architecture of the proposed hybrid OSN-VSN framework, namely, SOLVER i.e., Social OnLine and social VEhicular netwoRks;
2) We describe the SOLVER communication paradigm for (*i*) intra- and inter-VSN communications, as well as (*ii*) data redirection from OSN to VSN. The SOLVER communication framework acts a handover procedure from VSN to OSN, and vice versa, for communication management;
3) Security and privacy issues are addressed in SOLVER framework on different layers, thus

providing different security levels to both vehicles and drivers/passengers;

4) Numerical results assess the effectiveness of the proposed SOLVER framework that is based on a hybrid CS and P2P network architecture.

This paper is organized as follows. Section II presents a short overview of existing social-aware frameworks for vehicular networks. Section III introduces the SOLVER communication paradigm. Section IV describes the SOLVER network architecture, where we present the handover procedure from VSNs to OSNs, and vice versa. In Section V numerical results deal with the minimum transmission delay and the connectivity probability for the proposed framework. Finally, conclusions are drawn at the end of this paper.

II. Related works

Due to different features of VSNs and OSNs, both paradigms can be complementary to each other in order to overcome main limitations. For instance, as an open challenge, the limited life time of VSNs can be solved on relaying important information towards the OSN platform, by exploiting stable OSN social ties among members of a VSN. Also, the limited access to VSNs can be "bypassed" through a handover mechanism that switches and redirects important messages from VSN to OSN. At the same time, messages exchanged among the members of the same community in OSNs can be diffused among the members of a VSN, if OSN users also belong to a VSN community. This is expected to extend the diffusion of messages from OSN to VSN, providing enhanced network performance and a reduction of traffic load. Indeed, in OSNs, for a given communication pattern among users, the server load depends critically on the number of users assigned to a given server.

In the literature, there exist other social-aware frameworks that apply to wireless networks [7]–[11]. One of the main solutions is the architecture for the Internet of Things, with social networking, namely Social IoT, as described in [7]. In [8], Machado *et al.* propose a framework for distributed caching based on social and spatio-temporal features of OSN users. Pensa and Di Blasi [9] describe a formal framework for privacy self-assessment in OSNs. Zhang *et al.* [10] investigate a social-aware framework for smartphone ad-hoc networks, based on both user relationships in OSNs communities and wireless connections at the physical layer. Khan and Ghamri-Doudane [11] present SAVING, i.e., a socially-aware framework that provides distributed content caching to mobile users. Finally, Campolo *et al.* propose a social-enhanced 5G-based

framework for Vehicle-to-Everything communications (V2X) with the aim to exploit social relationships between vehicles and neighboring things [12].

Differently from existing frameworks, which are based on either OSNs or V2X scenarios only, SOLVER is the first hybrid platform that integrates OSNs with VSNs, in order to exploit the benefits coming from both two networks.

III. SOLVER Communication Paradigm

The SOLVER main goals can be summarized as follows:

1) SOLVER provides a seamless solution that integrates VSNs with OSNs such as Facebook, in order to generate an extended hybrid social network working both in centralized and distributed mode;
2) SOLVER allows the connection of isolated VSNs with always connected OSN communities in order to extend data dissemination into OSNs, and store important content that would be alternatively lost (i.e., **intra-VSN communications**);
3) SOLVER allows the connection of isolated VSNs among them, through social ties that exist among users belonging to both VSNs and OSNs communities (i.e., **inter-VSN communications**);
4) SOLVER allows redirection of data flow from OSNs towards selected nodes in a VSN, and data are disseminated according to a decentralized solution, as typical of VSNs (i.e., **OSN extension into VSNs**).

As known, VSNs present limited connectivity due to mobility and variable speed of vehicles, and opportunistic links are exploited in order to keep connectivity alive. However, there exist situations where vehicle-to-vehicle (V2V) links are not available (e.g., in a sparse traffic scenario with reduced vehicular density). In this regard, OSN ties can be exploited in order to cache relevant content from a VSN, whenever the connectivity links are not available anymore. Analogously, OSN ties that exist among users of the same community can be exploited in order to *bridge* two isolated VSNs, whenever OSN users are also VSN members. This occurs when the content of a VSN can be of interest also for another VSN. Finally, an OSN community can be virtually extended into a vehicular network scenario, allowing switching of traffic load from OSN to VSN. The following Subsection III-A and III-B present intra and inter-VSN communication paradigms, respectively, while Subsection III-C describes the "OSN extension into VSN" paradigm.

Fig. 7 depicts the schematic of the coexistence of OSNs with VSNs. We can distinguish the following social relationships i.e., (*i*) content-based social ties (CBS), (*ii*) driver-based social ties (DBS), and (*iii*) position-based social ties (PBS). CBSs are established between two nodes if they share common interests. A list of interests are broadcast by each vehicle based on driver/passenger profile. DBSs are established between two nodes if there exist social relationships between drivers/passengers of two neighboring vehicles. For instance, students of the same university driving to the campus can share common interests. Finally, PBSs are built between two nodes if they encounter each other according to spatio-temporal dependence (e.g., everyday along the same route). The formation of a VSN occurs among nodes that have social ties in common, such as CBS, PBS and DBS. Two VSNs (i.e., VSN_1 and VSN_2) share interests with their users via V2V links. Due to mobility constraints and transmission limitations, VSN_1 and VSN_2 are not connected to each other. Moreover, nodes of a VSN can belong to external OSN communities, and eventually be friends or present other social ties. As an instance, we suppose that in VSN_1 and VSN_2 blue and gray nodes belong to OSN community 1 and 2 too, respectively.

Generally, in VSNs we distinguish different content classes such as (*i*) safety, (*ii*) traffic management, and (*iii*) entertainment, each of them with dedicated requirements (i.e., data rate, reliability, and latency). Safety applications [13] require very fast content dissemination among members of the same community, and need spatio-temporal dependance (i.e., a safety message needs to be sent here and now). In this scenario, the message transmission occur first among neighboring vehicles, then is extended to furthest vehicles if necessary. Latency requirements are very high, as well as the reliability, meaning that a message needs to be sent as soon as a connectivity link is available (i.e., a social tie is built), while data rate requirement is low (i.e., low data rates to transmit a security message or warning). Differently, applications like traffic management (i.e., cooperative road awareness and control) show high requirements in terms of both latency and reliability, and data rate requirements more effective essentially depending on the data traffic to be transmitted. Finally, entertainment applications seek for low latency and reliability requirements, but need high data rate requirements.

According to different VSN content classes and requirements, we observe that “real-time” applications like safety applications prefer data dissemination over VSN P2P mode, also due to the message relevance among neighboring vehicles. Similar considerations apply to entertainment applications among vehicles, which share common content according to a spatio-temporal dependance. However, a few applications consider message redirection in case of connectivity

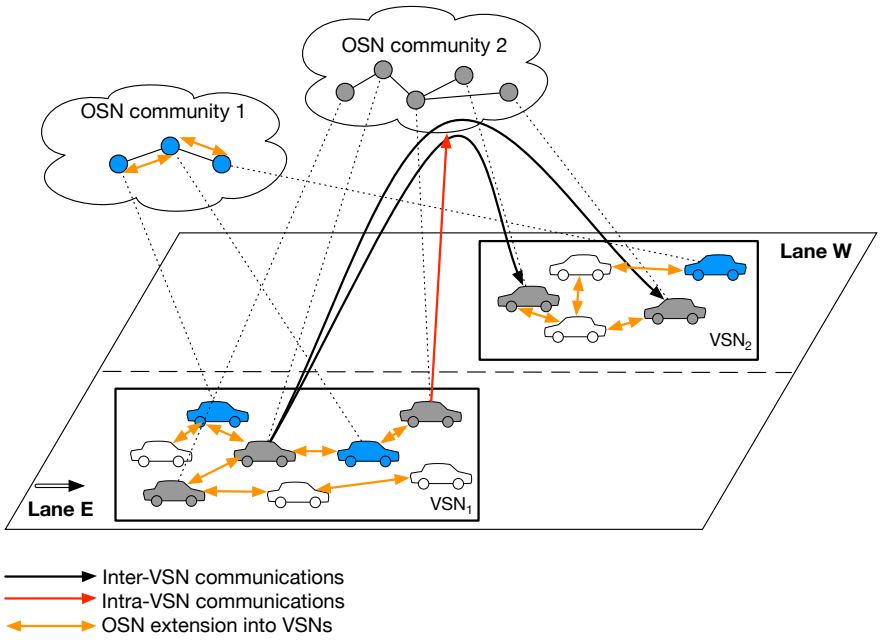


Fig. 1. Co-existence of OSNs and VSNs for inter, intra-VSN communications and OSN extension into VSN. Blue and grey vehicles belong to OSN community 1 and 2, respectively.

lack or lost; traditionally, in vehicular communications this is fixed through the *store-carry-and-forward* paradigm, so that a message will be forwarded as soon as a new link is available in the vehicular network. A similar approach is proposed in this paper, taking advantage of full available OSN connectivity links supported by a CS network architecture. Messages in a VSN can be redirected towards an OSN community, whenever no connectivity link is available for forwarding.

A. Intra-VSN Communications

In intra-VSN communications, relevant information can be cached and eventually shared among users of the same OSN community in order to keep alive the information generated in a VSN. Intra-VSN communications are built through OSN social ties of nodes belonging to VSNs. The aim is to cache relevant content of a VSN, which is expected being no longer available due to limited lifetime of connectivity links of vehicular scenarios. As an instance, a group of people all driving to a football game would like to share common interest not only during their journey to the stadium but also after the match has finished. In Fig. 7, gray vehicles in VSN_1 are also members of OSN community 2. In order to store relevant content generated in

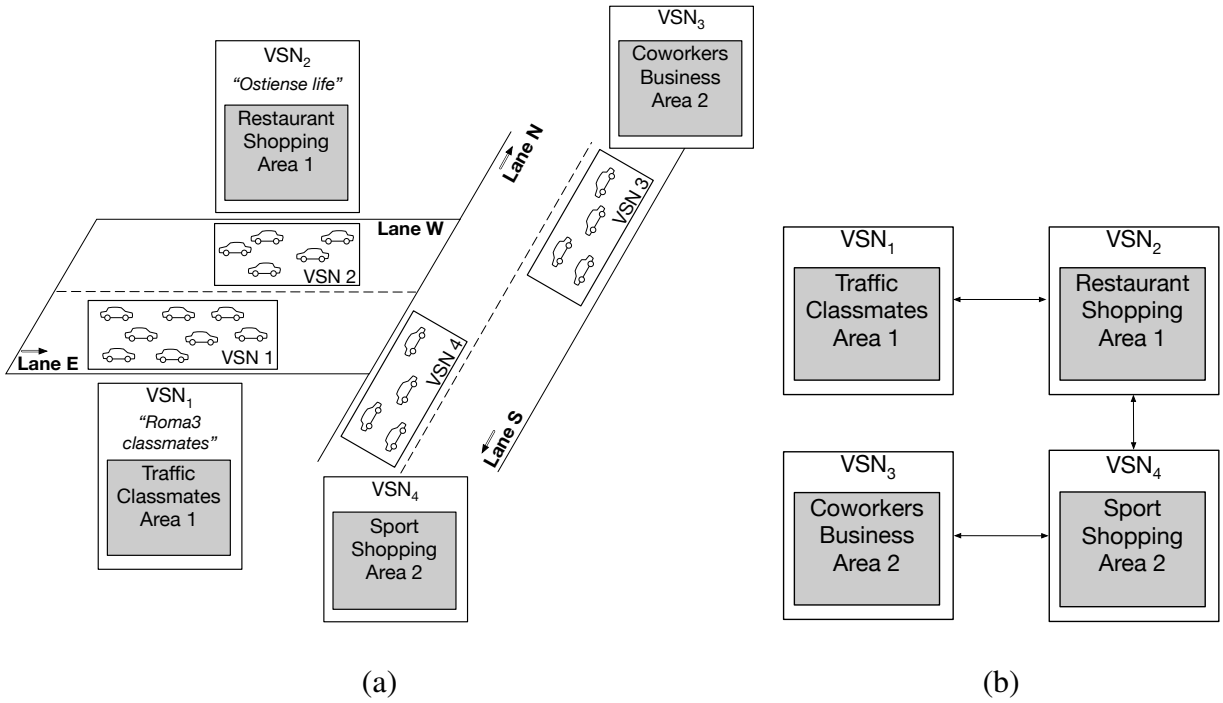


Fig. 2. (a) Tags of VSNs based on content, relationship, and positions. (b) Similarity ties among VSNs.

VSN_1, a cluster-head (CH) vehicle forwards it to OSN community 2 (see red arrow in Fig. 7), where it will be stored and kept available to other nodes.

Notice that a node is elected as cluster head (sometimes a.k.a hub node) based on its importance within the VSN. There exist several approaches that select a node as a cluster head, such as techniques based on graph theory metrics like centrality or betweenness. The importance of a node within the network is computed by each vehicle, according to a cloud-based architecture. Furthermore, an information message shared in a VSN is assumed as relevant if its time-to-live has not expired yet and it is transmitted by a CH vehicle. This assumption allows to cache all information messages shared in the network.

B. Inter-VSN Communications

Inter-VSN communications are built through OSN ties in order to bridge two isolated VSNs sharing related topics i.e., the content of a VSN can be of interest also to another VSN. For this purpose, VSNs need to be initially tagged by the users with relevant topics and keywords. A similarity check of keywords and tags of different VSNs allows to identify if two VSNs have common or similar topics. Once detected if two VSNs (i.e., VSN_1 and VSN_2) are related

networks, the "virtual bridge" linking the two VSNs is built through the social ties of users in VSN_1 with users in VSN_2, which are also members of OSN community 2.

Let us consider a vehicular scenario as the one depicted in Fig. 8(a). Several VSNs exist (i.e., from VSN_1 to VSN_4), each tagged with a set of keywords. Notice that tags of a VSN are related to its main attributes and criteria that allow a VSN to be formed i.e., content, relationship and position [3]. For instance, VSN_1 represents the community of classmates attending classes at Roma Tre University (namely, Roma3 classmates community). The keywords of VSN_1 represent the main topics discussed among its members e.g., a student may be interested in traffic conditions to reach the university ("traffic" tag), as well as information about professors' office hours ("classmates" tag). VSN_1 is also tagged according to its location (i.e., Area 1, the zone where vehicles form VSN_1).

VSN_2 is tagged by the keywords "restaurant" and "shopping", and it is located according to "Area 1" position. VSN_2 represents the community of vehicles sharing content about entertainment activity in "Ostiense" neighborhood (namely, Ostiense life), that is located in Area 1. It follows that the content shared in VSN_2 can be of interest also to users in VSN_1, since they have a common tag i.e., Area 1. According to the tags in Fig. 8(b), VSN_1 and VSN_2 have one attribute in common (i.e., Area 1). It follows that VSN_1 and VSN_2 are related networks, and users in VSN_1 can be interested in content discussed in VSN_2, and vice versa.

C. OSN Extension into VSNs

The SOLVER framework allows to redirect shared data from an OSN community towards a VSN. This occurs if OSN members also belong to a VSN community. Traditionally, data shared in an OSN community are transmitted via CS mode, and can affect the servers in case of data traffic overflow. Data can be then redirected to users of a VSN via P2P mode, and transmissions will occur according to a hybrid CS-P2P mode. Indeed, if two OSN users are also members of the same VSN, they can communicate to each other via V2V instead of CS mode. Communications via V2V involve only the two users (i.e., direct communication), while communications in CS mode involve one or more servers of the OSN community, thus stressing the overall system. As it will be shown in Section V, the benefits of the OSN extension into VSNs are mainly in terms of a reduced transmission delay.

To summarize, Algorithm 1 shows the pseudo-code of the SOLVER communication paradigm. Given the graphs of VSN and OSN i.e., G_V and G_O, respectively, where $V_{V/O}$ is the set of

nodes in the VSN/OSN, and $E_{V/O}$ is the set of edges in VSN and OSN graphs, we assume the presence of at least two VSN communities (i.e., VSN_1 and VSN_2). Also, in OSN a server node s_O is responsible for CS communication mode. In case of intra-VSN communications, a new connectivity link ℓ will be established between node u_i and s_O in the OSN, if node u_i experiences a low connectivity link (i.e., $Connectivity\_prob(u_i) < \rho$) and needs a handover to OSN.

In case of inter-VSN communications, the similarity check between at least two VSN communities is provided, i.e., $Similarity\_check(VSN_1, VSN_2)$, and if positive, it allows to establish a new connectivity link in OSN domain between node u_i and u_j, which belong to both OSN and VSN, but in different vehicular communities. Finally, if a couple of nodes u_i and u_j belong to both VSN and OSN, then a new connectivity link is built in the VSN among such nodes. This latter approach represents the case of "OSN extension into VSN".

IV. SOLVER Network Architecture

The integration of OSNs with VSNs in a unique platform is provided through the SOLVER network architecture, which is organized into four components i.e., (*i*) the SOLVER Mobile Platform, (*ii*) the SOLVER Cloud Platform, (*iii*) the SOLVER Web Application, and (*iv*) a transversal SOLVER Security and Trust Platform.

The SOLVER Mobile Platform allows the handover management from VSNs to OSN communities, and vice versa. Moreover, it is responsible of collection and storage of relevant content transmitted by a CH node. The SOLVER Cloud Platform represents the core of SOLVER architecture since it is the interface to both VSN and OSN systems, so that vehicles/users authenticate and access to OSN/VSN community, respectively. The SOLVER Security and Trust Platform takes care of security and trust based on well-known encryption mechanisms of both OSN and VSN systems. Finally, as the name expresses, the SOLVER Web Application provides a web application that shows the relevant content sent by a CH node from a VSN community, directly on the OSN community website.

Due to the hybrid framework that allows the coexistence of VSNs and OSNs in a common platform, both SOLVER Mobile platform and the SOLVER Cloud platform show two separated sides, dedicated to (*i*) VSNs and (*ii*) OSNs, respectively. This separation is needed to accomplish the handover mechanism, authentication and access of users to OSN/VSN. On the other hand, the SOLVER Web Application exists in case of intra-VSN communications. We can then conclude

Algorithm 1: SOLVER pseudocode in case of (a) intra-VSN, (b) inter-VSN, and (c) OSN extension into VSNs communication modes.

Input:

$G_V = \{V_V, E_V\}$ ▷ VSN graph

$G_O = \{V_O, E_O\}$ ▷ OSN graph

$VSN_1, VSN_2 \subset G_V$, ▷ VSN communities

with $VSN_1 \neq VSN_2$, $VSN_{1,2} = \{V_{V1,2}, E_{V1,2}\}$

$s_O \in V_O$ ▷ OSN server

ρ ▷ Threshold for handover decision

Output: ℓ ▷ New connectivity link

(a) **while** $(u_i \in V_V \wedge u_i \in V_O)$ **do**

  if $Connectivity\_prob(u_i) < \rho$ **then**

    $e_{(u_i,s_O)} \in E_O$ ▷ Connectivity link in OSN between u_j and s_O

    $\ell \leftarrow 1$

  else

    $\ell \leftarrow 0$

(b) **while** *Similarity_check*$(VSN_1, VSN_2) == 1$ **do**

  if $\Big[(u_i \in V_{V1}) \ \wedge \ (u_i \in V_O)\Big] \cup \Big[(u_j \in V_{V2}) \ \wedge \ (u_j \in V_O)\Big]$ **then**

    $e_{(u_i,u_j)} \in E_O$ ▷ Connectivity link in OSN between u_i and u_j

    $\ell \leftarrow 1$

  else

    $\ell \leftarrow 0$

(c) **if** $\Big([u_i, u_j] \in V_O \wedge [u_i, u_j] \in V_V\Big)$ **then**

  $e_{(u_i,u_j)} \in E_V$ ▷ Connectivity link in VSN between u_j and u_j

  $\ell \leftarrow 1$

else

  $\ell \leftarrow 0$

that the proposed SOLVER network architecture acts differently in case of (*i*) intra, (*ii*) inter-VSN communications, and (*iii*) OSN extension into VSN paradigms.

In case of intra-VSN communications (see white circles in Fig. 9 that indicate the routing of data flow), the SOLVER Mobile Platform gathers the relevant content generated by vehicles in a VSN, to be forwarded towards a given OSN community, where users of a VSN have social

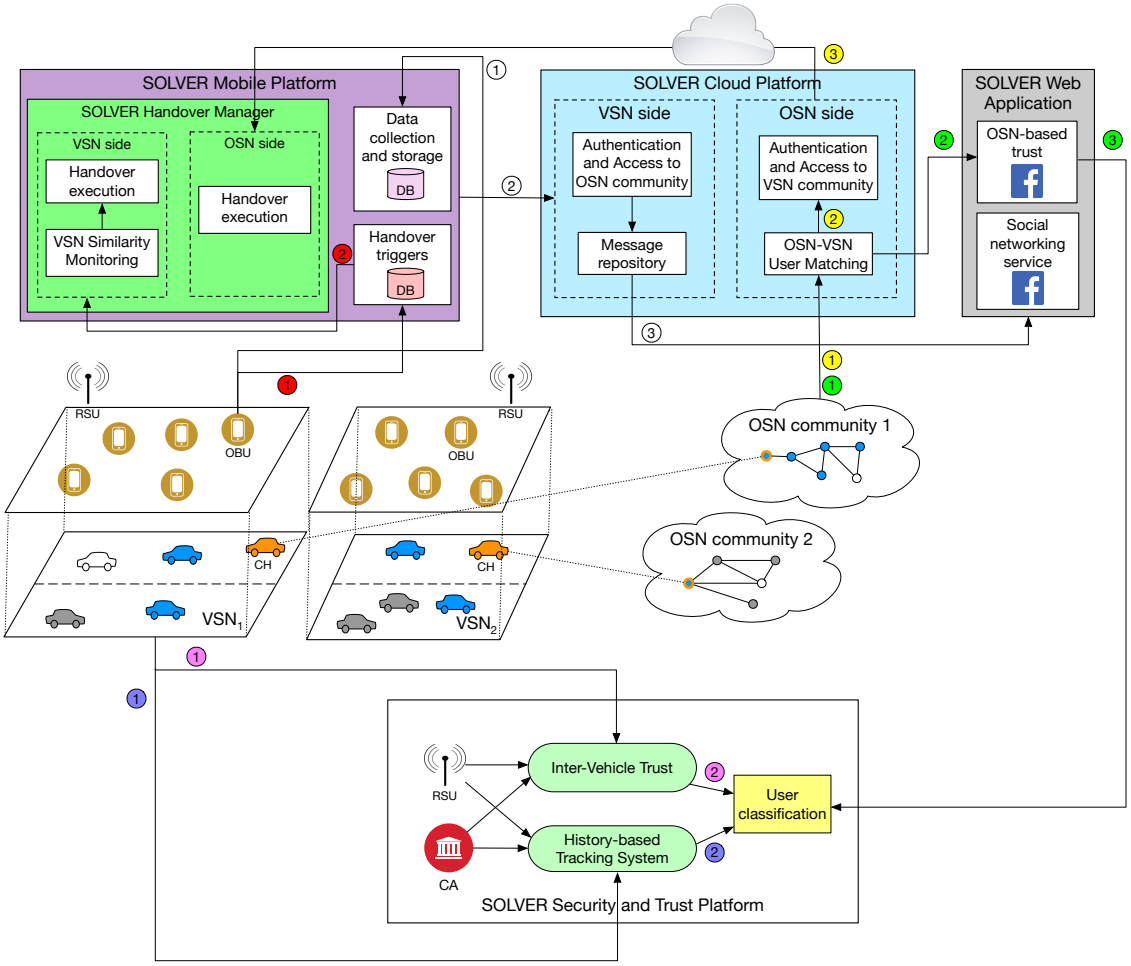


Fig. 3. SOLVER network architecture. White, red, and yellow circles refer to intra-VSN, inter-VSN communications, and OSN extension into VSN paradigms, respectively. Purple, pink and green circles refer to the security management in case of inter-vehicle trust, history-based tracking, and OSN-based trust, respectively. The arrows indicate the data flows.

ties. In Fig. 9, due to existing OSN profiles of drivers/passengers, we assume that each vehicle in a VSN, equipped with an On-Board Unit (OBU), can have social ties with other nodes in an OSN community. Specifically, blue (gray) vehicles in VSN_1 have social ties in OSN community 1 (2), as well as blue (gray) vehicles in VSN_2 have social ties in OSN community 1 (2). The CH node connects with the SOLVER Mobile Platform to store relevant content in the data collection and storage database (see the arrow with white circle 1). Stored content is then transmitted to the SOLVER Cloud Platform (see the arrow with white circle 2), which is comprised of two parts i.e., (*i*) the VSN side, and (*ii*) the OSN side, that are referred to the networks the data are coming from.

The SOLVER Cloud Platform provides a central coordinating platform to store the content to be eventually posted on an OSN community, previously selected based on OSN user profiles. So, in case of intra-VSN communications, stored data will be sent to the VSN side of the SOLVER Cloud Platform, where it will be done the authentication and access of the CH node to the OSN community it belongs to, and data will be stored in the message repository database. Finally, the SOLVER Web Application is deployed as a web application to provide a social networking service, which assists users to view, post and comment on relevant content from the VSN CH, directly on the OSN community website (see the arrow with white circle 3). Notice that the SOLVER Web Application also provides a trust level based on OSN user profiles. This aspect is exploited together with the SOLVER Security and Trust platform.

In case of inter-VSN communications, the data flow occurs according to the arrows with red circles, as indicated in Fig. 9. Again, the CH node is responsible for transmission of relevant content and handover decision towards a selected VSN, based on physical triggers that may occur, such as low connectivity or loss among VSN members (see the arrow with red circle 1). The CH node transmits the handover request towards another VSN, to be selected according to the VSN similarity check (see the arrow with red circle 2). Specifically, the handover trigger database pushes the SOLVER Handover Manager to initiate an inter-VSN handover procedure. The VSN Similarity Monitoring makes the similarity check of neighboring VSNs in order to detect one or more candidate VSNs for inter-VSN communications (i.e., handover execution). Notice that, although it is not the main goal of this paper, we expect that in the similarity check two VSNs are defined as related networks if at least one tag is in common to each other.

Finally, in the OSN extension into VSN paradigm, users in an OSN community connect to the SOLVER Cloud Platform, where the OSN-VSN User Matching toolbox checks for available VSNs whose members are also OSN users (see the arrow with yellow circle 1). After detecting a potential VSN for extending the OSN community, the SOLVER Cloud Platform allows the OSN user to authenticate and access a chosen VSN, according to known authentication methods of vehicular networks (see the arrow with yellow circle 2). The SOLVER Handover Manager in SOLVER Mobile platform is responsible to execute the handover from OSN to VSN (see the arrow with yellow circle 3). Data messages are then forwarded via V2V mode, according to the P2P architecture as typical of VSNs.

In all the communication modes available in SOLVER, security and trust are supported by the SOLVER Security and Trust Platform that guarantees different security levels. First, driver/

passenger's honesty factor is provided through their OSN profiles. After matching OSN/VSN user profiles (see the arrow with green circle 1), the system checks the OSN-based trust (see the arrow with green circle 2) in order to classify a user as good, bad or compromised (see the arrow with green circle 3). Authentication of the users relies on well-defined encryption and security mechanisms already defined in OSNs [14] and vehicular networks [15]. Security level on the vehicle itself is provided through (*i*) an inter-vehicle trust that recommends vehicle's trust based on the interactions among vehicles, and (*ii*) a history-based tracking system that checks for past vehicle's positions [6]. As an instance, a vehicle that uses to move in a given area in working days is expected to be trusted since its mobility pattern is periodic. Notice that the SOLVER Security and Trust Platform involves not only vehicles, but also RSUs and CA.

V. Numerical results

In this section, we present numerical results obtained in MatLab environment, and expressed in terms of (*i*) minimum transmission delay that occurs in SOLVER in case of data redirection from VSN to OSN and vice versa, and (*ii*) probability of connectivity of nodes in a VSN in case of handover from VSN to OSN.

As early described, the SOLVER framework is comprised of both CS and P2P modes. Generally, in OSNs data transmission occurs according to CS protocol, and the minimum transmission delay is linearly proportional to the number of recipient nodes. On the other hand, in a VSN, data transmission is mainly based according to the P2P network architecture, where each vehicle (i.e., peer) can retransmit messages once received. Notice that P2P mode works in case of all VSN nodes are connected to each other's.

Let us consider N as the number of users in an OSN community, and n as the number of peers in a VSN. In the OSN, at least one server is available for message exchanges. Table II collects the main parameters used in the numerical results. In case of connectivity switching from OSN to a VSN (i.e., messages are transmitted according to a CS configuration in OSN, and then they are disseminated within a VSN according to P2P), SOLVER allows to reduce the minimum transmission delay, as depicted in Fig. 10(a) (see black curves). For $N > n$, the transmission delay of the server in the OSN will depend on $(N - n)$ nodes, while n peers will be receiving data according to P2P. It follows that for $(N > n)$, the minimum transmission delay will be linear as the CS trend. The CS and P2P curves are shown as benchmarks, respectively as highest and lowest values of the transmission delay. Indeed, in case of pure OSN (green curve),

TABLE II

PARAMETERS USED IN THE NUMERICAL RESULTS

Parameter	**Value**
$N = [1, 50]$	Number of nodes in OSN
$n = [1, 50]$	Number of nodes in VSN
Packet size	1000 Byte
Peer upload rate	1 Mbit/s
Server upload rate	2 Mbit/s
Minimum download rate per node	4 Mbit/s

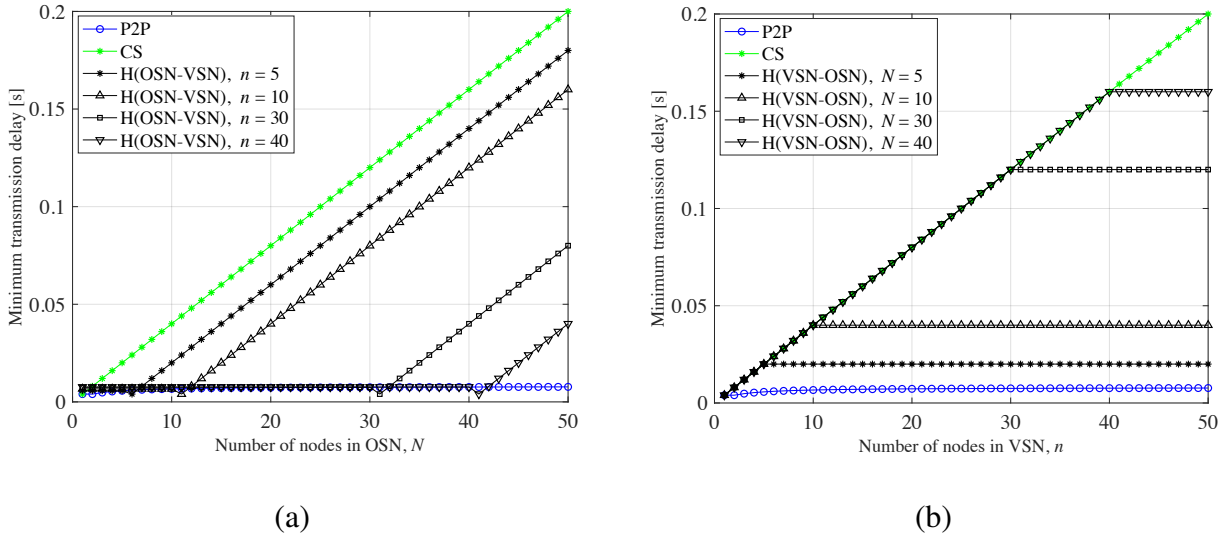
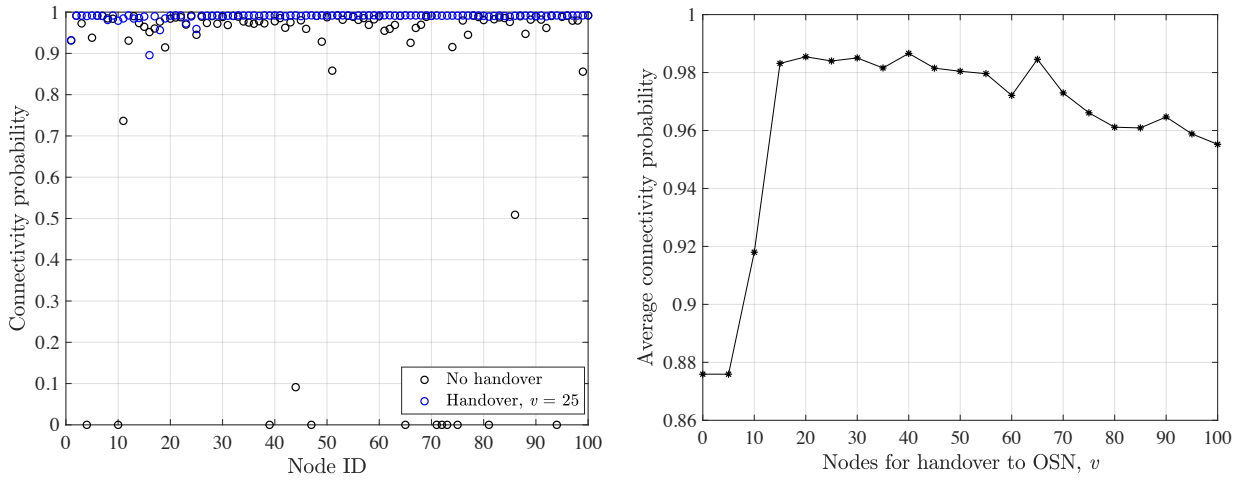


Fig. 4. Comparison of the minimum transmission time delay vs. number of nodes in case of pure OSN (i.e., CS), pure VSN (i.e., P2P), and hybrid architecture in case of (a) OSN-VSN and (b) VSN-OSN handover.

the system experiences highest delay, while it is reduced whenever packets are also redirected towards a number of peers in VSNs. Highest the peers, lowest the transmission delay, while preserving data forwarding.

On the other side, when $N \leq n$, data transmission will follow P2P mode for n nodes in the VSN. Depending on the number of peers n in a VSN to whom messages are disseminated, we observe a reduced transmission delay w.r.t. both a pure CS and a P2P architecture. The delay is constant for a given number of nodes acting in P2P mode, and then follows the CS behavior. Specifically, Fig. 10(a) depicts the behavior of the hybrid OSN-VSN approach for a different



(a) (b)

Fig. 5. (a) Connectivity probability for a given node in the VSN, in case of (*i*) no handover, and (*ii*) handovers executed to the OSN due to the presence of $n = 25$ nodes with OSN connectivity. (b) Average connectivity probability in the VSN versus the number of nodes n with OSN connectivity.

number of peers in a VSN (i.e., n), versus the number of users in the OSN community. If $n = 0$, the system overlaps with a pure CS architecture (i.e., no switching from OSN to VSN). For increasing n, the minimum transmission delay is approximately constant till n, then follows the CS trend.

Similar considerations apply in Fig. 10(b) in case of handover from VSN to OSN (as for intra- and inter-VSN communications). In this case, the minimum transmission delay is computed versus the number of peers in the VSN, and again the CS/P2P curves are plotted as benchmarks. The transmission delay in the VSN will depend on $(n - N)$ peers (in case $n > N$), while N users will keep on downloading the packet according to CS mode in OSN. We observe a linear behavior following the CS curve for $N \leq n$, while a constant trend with lower delay than the CS mode, as long as the number of nodes in VSN are involved in the transmission task (for $N > n$). Higher the number of nodes N is in the OSN, higher the transmission delay is, as compared to pure VSN scenario. Of course, this provides a benefit if we consider the availability of connectivity in OSNs.

Finally, we assessed the SOLVER framework in terms of probability of connectivity of a node in a VSN community. As known, due to mobility, V2V links become weak and disconnections may occur in the vehicular network. Exploiting the availability of OSN connectivity links, we

expect an increase of connectivity per node. In our simulations, we considered a VSN comprised of $V = 100$ vehicles, each one with a given number of neighbors to whom share messages, with different contact time. It has been established that the duration of the contacts among vehicles follows the power law distribution [16], and the probability that a contact duration X is greater than a given time x is a complementary Cumulative Distribution Function i.e., $P(X > x)$. Then, the probability that a vehicle is in connectivity to another node depends on the time they are in contact to each other. If $X > x$, then the vehicles will have a connectivity probability that is not null. On the contrary, in case of connectivity links between nodes in the same OSN community, they will have higher connectivity probability, as we assumed that a service in a OSN is expected as always available and accessible.

To allow connectivity switching from VSN to an OSN community, we assumed v nodes in VSN also have an OSN profile i.e., $v < V$ nodes belong to both OSN and VSN. Such nodes can establish links with other vehicles that belong to the same OSN community via OSN connectivity, with a connectivity probability that depends on the contact time duration. It follows that the presence of driver/passengers with OSN user profiles allows to increase the connectivity links in the overall VSN. Specifically, the average degree in the initial network configuration will be increasing due to the presence of nodes for handover from VSN to OSN. Fig. 11 depicts the connectivity probability versus different node IDs, in case of (*i*) no nodes with potential OSN links, and (*ii*) v nodes with OSN links for handover to OSN. This represents the probability of having at least a connectivity link; in case of multiple available links (i.e., a vehicle with several connectivity links), Fig. 11 shows the link with highest probability. As expected, we observe an increase of connectivity with SOLVER, w.r.t. the trend of no handover. In Fig. 11(a), we simulated $v = 25$ vehicles as potential nodes for handover to OSN, and we notice 11 nodes have a null connectivity probability (black markers), which on average increases in case of handover to OSN (blue markers). Notice that a few fluctuations of connectivity probability in case of handovers (i.e., connectivity higher for no handover than the case of handovers to OSN) may occur, and are mainly due to the availability of links with higher contact time in the vehicular network. Fig. 11(b) depicts the average connectivity probability in the VSN, versus the number of nodes v that can connect to the OSN and then perform handovers. We observe a high increase of the average connectivity probability for low values of v (i.e., $v < 15$), while the trend shows smooth variations for $v \geq 15$. For $v > 50$, small reductions of the connectivity probability are observed on average, meaning that increases of v higher than 50 do not necessary provide benefit

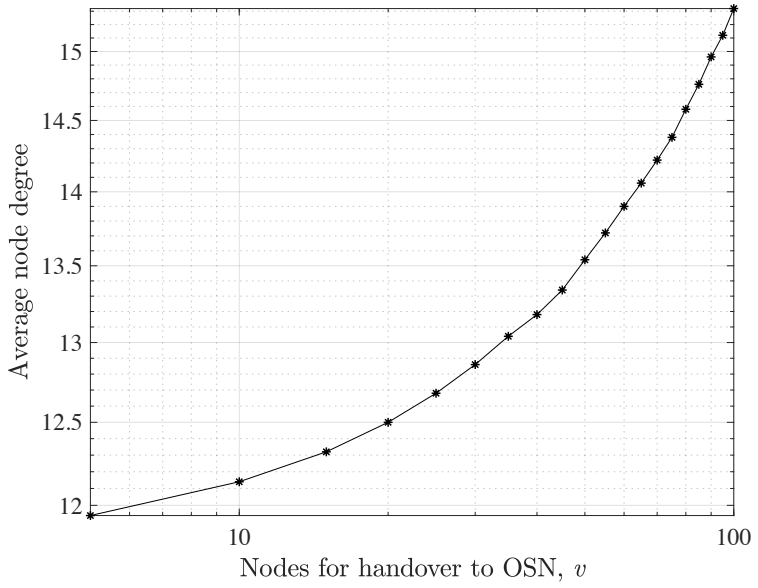


Fig. 6. Average node degree versus the number of nodes v with OSN connectivity for potential handovers.

to the overall network. Finally, Fig. 12 depicts the average node degree in the VSN versus the number of vehicles v with OSN connectivity for potential handovers. The trend is increasing with v, meaning that new connection links are built towards the OSN. However, based on the results in Fig. 11(b), new links to the OSN do not necessary guarantee best connectivity probability as it also depends on the contact duration of the links.

VI. Conclusions

In this paper, we have presented SOLVER i.e., a framework that integrates OSNs with VSNs, providing benefits to both networks. SOLVER arises due to the needs of reducing connectivity holes and the limited service of VSNs. At the same time, SOLVER allows the redirection of traffic load from OSN communities toward specific VSNs whose users are also members of OSNs, in order to reduce the overall load of the system and balancing the loads among OSN servers.

The SOLVER network architecture has been described for the support of different communication paradigms, while guaranteeing security and trust to different network entities (i.e., vehicles and drivers/passengers). Analysis of the transmission delay in the hybrid OSN-VSN platform proves how effective SOLVER is, providing a reduced time delay mainly w.r.t. traditional OSNs. Finally, connectivity increases and is guaranteed due to handovers in inter-VSN communications.

Anna Maria Vegni (A'07-M'15-SM'16) is a non-tenured Assistant Professor of Telecommunications with the Department of Engineering, Roma Tre University (Italy). She received the Laurea degree (*cum laude*) in Electronics Engineering and the Ph.D. degree in Biomedical Engineering, Electromagnetic, and Telecommunications from Roma Tre University, in 2006 and 2010, respectively. In 2009, she was a visiting researcher with the Multimedia Communication Laboratory, Department of Electrical and Computer Engineering, Boston University, Boston, MA, USA, where she worked on vehicular networking and optical wireless communications. Since 2010, she has been in charge of the Telecommunications Networks Laboratory course at Roma Tre University. Her research interests include vehicular social networking, visible light communications, and nanocommunications. She is involved in several EU programs and organization committees of international conferences. She is an associate editor for AD HOC NETWORKS, JNCA, and NANOCOMNET Elsevier journals. In March 2018, she got the Italian Habilitation (Abilitazione Scientifica Nazionale) for Associate Professorship in Telecommunication Engineering (SC: 09/F2; SSD: ING-INF/03).

Valeria Loscrí is a permanent researcher of the FUN Team at Inria Lille-Nord Europe since Oct. 2013. From Dec. 2006 to Sept. 2013, she was Research Fellow in the TITAN Lab of the University of Calabria, Italy. She received her MSc and PhD degrees in Computer Science in 2003 and 2007, respectively, from the University of Calabria. Her research interests focus on heterogeneous communication technologies and cooperation of heterogeneous devices. She has been involved in the activities of several European Projects (FP7 EU project VITAL, the FP6 EU project MASCOT, etc.), Italian and French projects. She is in the editorial board of Elsevier ComNet, JNCA, IEEE Trans. on Nanobioscience. She has been guest editor for a Special Issue in Elsevier Ad Hoc Networks and she has been editor of the book "Vehicular Social Networks" published by CRC Taylor & Francis Group, in March 2017 and "Management of Cyber Physical Objects in the Future Internet of Things" published by Springer. Since 2015 she is member of the Committee for Technological Development at Inria Lille-Nord Europe. Since 2016, she is Scientific European Responsible for Inria Lille-Nord Europe.

Abderrahim Benslimane is Full Professor of Computer-Science at the Avignon University/France. He has more than 150 refereed international publications. He is EiC of Multimedia Intelligence and Security Journal, Area Editor of Wiley Security and Privacy Journal and editorial member of IEEE Wireless Communication Magazine and Elsevier Ad Hoc. He serves as General-Chair of the IEEE WiMob since 2008; he lunched and serves as General-Chair of MoWNet, since 2011. He served as a Symposium co-chair/leader in many IEEE international conferences such as ICC, Globecom, AINA and VTC. He is Chair of the IEEE Communication Society TC of Communication and Information Security.

REFERENCES

[1] V. Arnaboldi, A. Guazzini, and A. Passarella, "Egocentric online social networks: Analysis of key features and prediction of tie strength in facebook," *Computer Communications*, vol. 36, no. 10, pp. 1130 – 1144, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366413000856

[2] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[3] A. M. Vegni and V. Loscri, "A Survey on Vehicular Social Networks," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2397–2419, 2015.

[4] T. Weil, "VPKI Hits the Highway: Secure Communication for the Connected Vehicle Program," *IT Professional*, vol. 19, no. 1, pp. 59–63, Jan 2017.

[5] L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based Collaborative Privacy Management in Online Social Networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 48–60, Jan 2019.

[6] C. A. Kerrache, N. Lagraa, R. Hussain, S. H. Ahmed, A. Benslimane, C. T. Calafate, J. Cano, and A. M. Vegni, "TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[7] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT), When social networks meet the Internet of Things: Concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594 – 3608, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128612002654

[8] K. Machado, A. Boukerche, E. Cerqueira, and A. A. F. Loureiro, "A socially-aware in-network caching framework for the next generation of wireless networks," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 38–43, Dec 2017.

[9] R. G. Pensa and G. D. Blasi, "A privacy self-assessment framework for online social networks," *Expert Systems with Applications*, vol. 86, pp. 18 – 31, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417417303767

[10] Y. Zhang, L. Song, C. Jiang, N. H. Tran, Z. Dawy, and Z. Han, "A social-aware framework for efficient information dissemination in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 174–179, January 2017.

[11] J. A. Khan and Y. Ghamri-Doudane, "Saving: socially aware vehicular information-centric networking," *IEEE Communications Magazine*, vol. 54, no. 8, pp. 100–107, August 2016.

[12] C. Campolo, A. Molinaro, and A. Iera, "A reference framework for social-enhanced Vehicle-to-Everything communications in 5G scenarios," *Computer Networks*, vol. 143, pp. 140 – 152, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912861830495X

[13] H. Nguyen-Minh, A. Benslimane, and M. Radenkovic, "Social delay tolerant approach for safety services in vehicular networks," in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug 2015, pp. 1199–1204.

[14] C. Fan, Y. Tseng, J. Huang, S. Chen, and H. Kikuchi, "Multireceiver predicate encryption for online social networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 2, pp. 388–403, June 2017.

[15] A. M. S. Abdelgader, F. Shu, W. Zhu, and K. Ayoub, "Security challenges and trends in vehicular communications," in *2017 IEEE Conference on Systems, Process and Control (ICSPC)*, Dec 2017, pp. 105–110.

[16] Y. Li, D. Jin, Z. Wang, L. Zeng, and S. Chen, "Exponential and power law distribution of contact duration in urban vehicular ad hoc networks," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 110–113, Jan 2013.

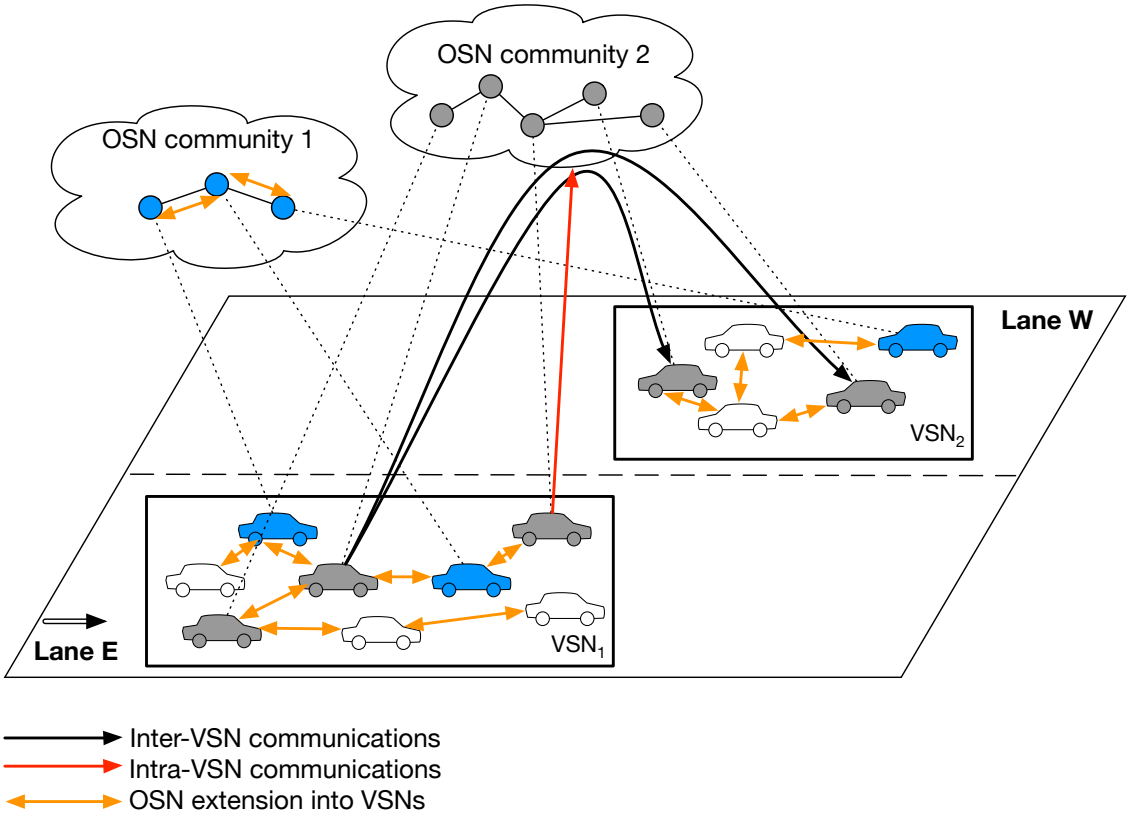


Fig. 7. Co-existence of OSNs and VSNs for inter, intra-VSN communications and OSN extension into VSN. Blue and grey vehicles belong to OSN community 1 and 2, respectively.

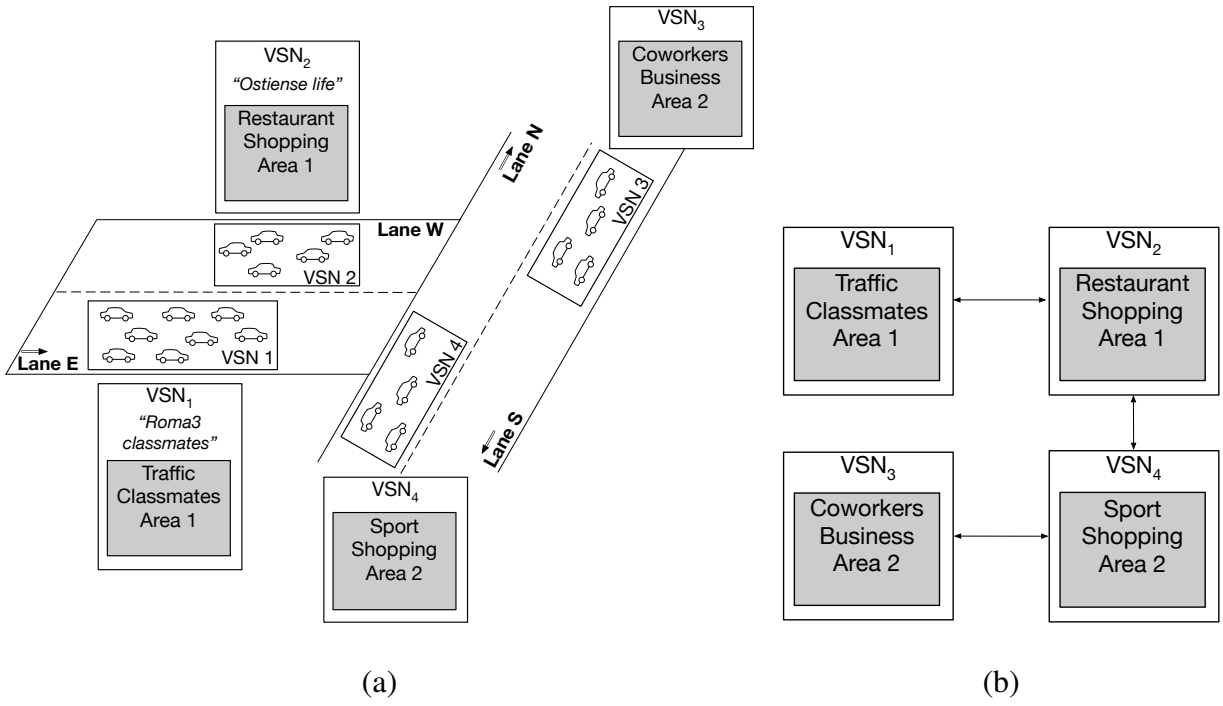


Fig. 8. (a) Tags of VSNs based on content, relationship, and positions. (b) Similarity ties among VSNs.

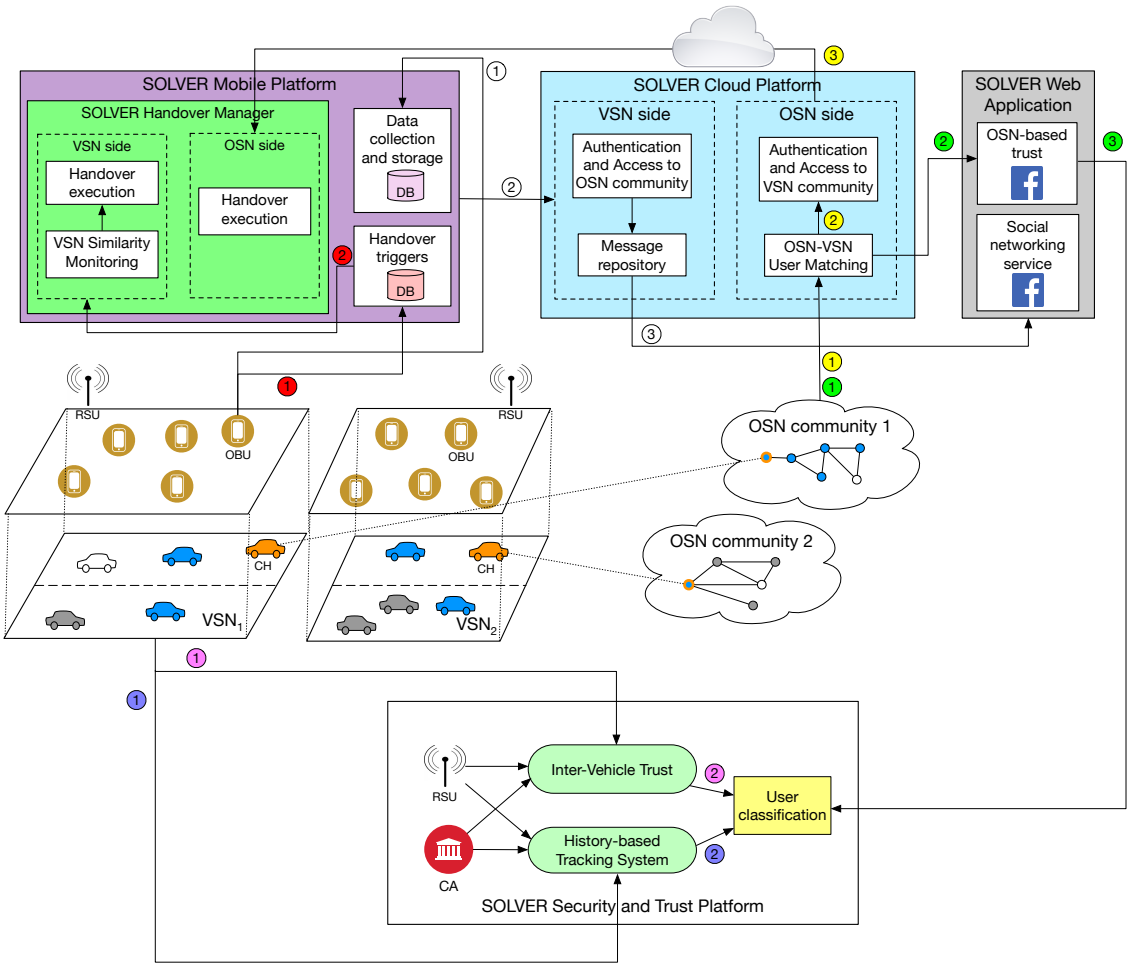


Fig. 9. SOLVER network architecture. White, red, and yellow circles refer to intra-VSN, inter-VSN communications, and OSN extension into VSN paradigms, respectively. Purple, pink and green circles refer to the security management in case of inter-vehicle trust, history-based tracking, and OSN-based trust, respectively. The arrows indicate the data flows.

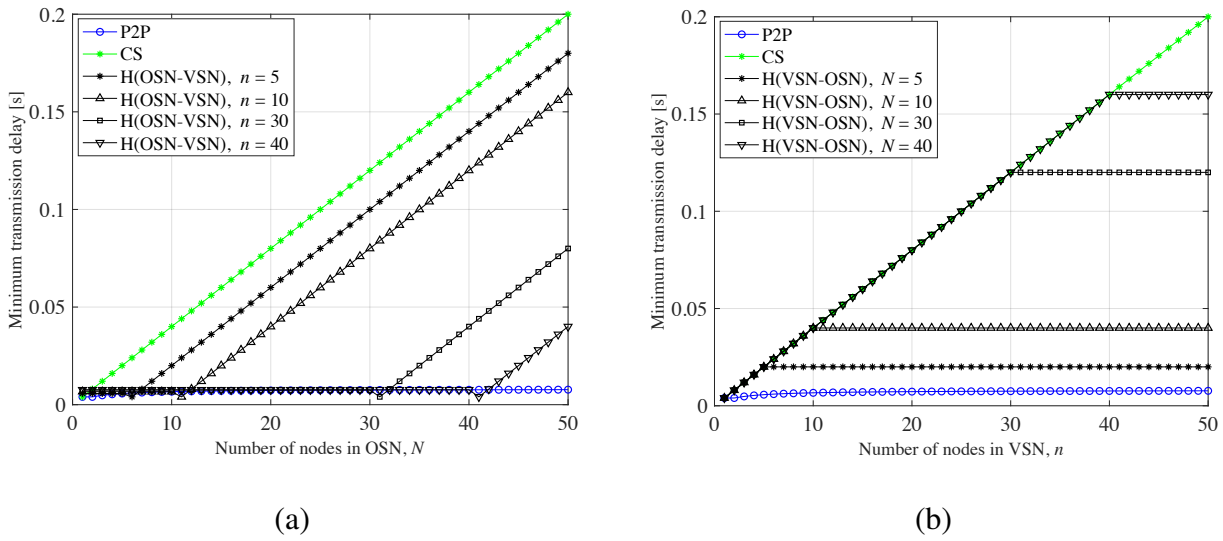
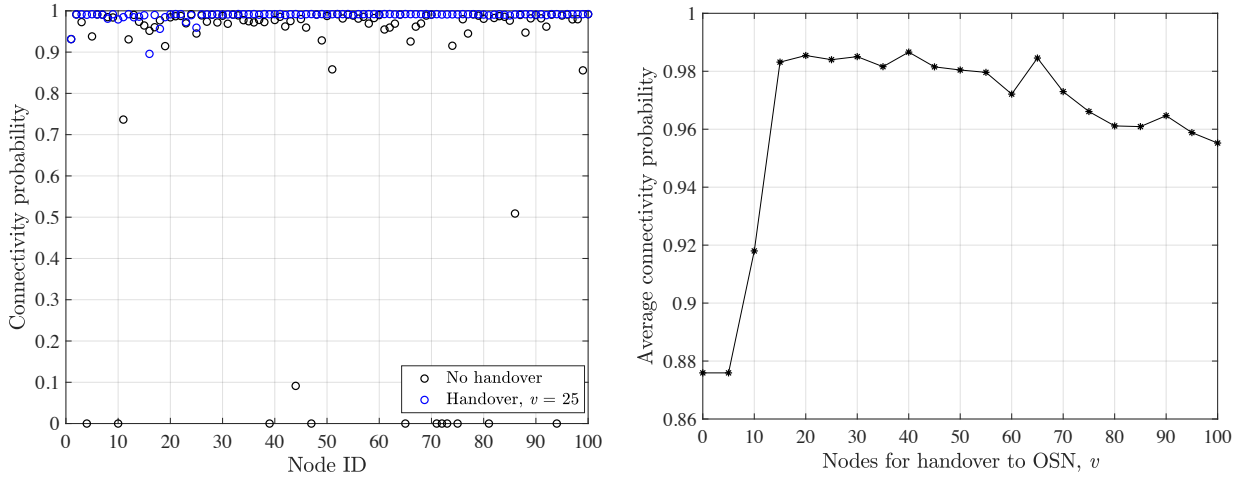


Fig. 10. Comparison of the minimum transmission time delay vs. number of nodes in case of pure OSN (i.e., CS), pure VSN (i.e., P2P), and hybrid architecture in case of (a) OSN-VSN and (b) VSN-OSN handover.



(a) (b)

Fig. 11. (a) Connectivity probability for a given node in the VSN, in case of (*i*) no handover, and (*ii*) handovers executed to the OSN due to the presence of $n = 25$ nodes with OSN connectivity. (b) Average connectivity probability in the VSN versus the number of nodes n with OSN connectivity.

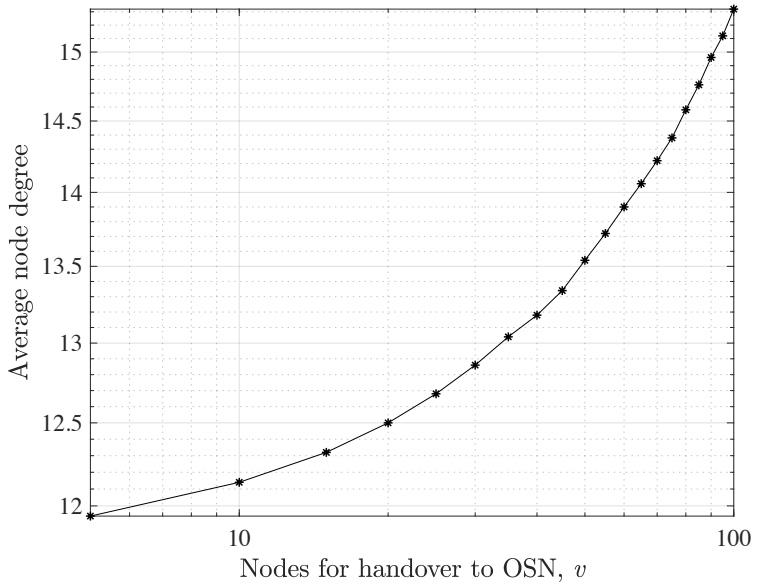


Fig. 12. Average node degree versus the number of nodes v with OSN connectivity for potential handovers.