EAI Endorsed Transactions
on Cloud Systems

Research Article ICST.ORG

Social Aspect of Vehicular Communications

Leandros A. Maglaras[1,*], Efstathios Stathakidis[1], Jianmin Jiang[1]

[1]Department of Computing, University of Surrey, Guildford, UK

Abstract

The interconnection of devices is expected to grow and to incorporate systems that used to be isolated. As the vehicle evolves from a simple transport machine to an intelligent entity that collects information from the environment and uses it in order to take decisions in real time, it is becoming an active member of a smart city. The integration of vehicular communications with smartphones helps vehicles connect with each other and take decisions that improve driving in terms of safety, reduced fuel consumption and comfort. The social behavior of drivers is an asset that can be used in order to predict their mobility in a city and to produce novel algorithms that can cope with these aspects in an efficient way. In this article, we present a social perspective of ad hoc vehicular networks and propose novel ranking, clustering and routing methods. We also discuss security issues that arise from the interconnection of vehicles.

Keywords: Social networks, vehicular ad hoc networks, LTE, intelligent transportation systems, Internet of Vehicles(IoV)

Received on 27 November 2014, accepted on 20 January 2015, published on 23 February 2015

doi: 10.4108/cs.1.1.e6

1. Introduction - The Internet of Things in vehicular communications

The Internet of Things (IoT) is an emerging topic that refers to the interconnection of devices from different environments [1](e.g. sensors, industrial equipment, smart phones, vehicles). As $WiFi$ and $4G-LTE$ wireless Internet access continues to grow, the evolution towards ubiquitous information and communication networks is already evident. Internet of Vehicle (IoV) technology refers to dynamic mobile communication systems that communicate between vehicles and public networks using $V2V$ (vehicle-to-vehicle), $V2R$ (vehicle-to-road), $V2H$ (vehicle-to-human) and $V2S$ (vehicle-to-sensor) interactions. It enables information sharing and the gathering of information on vehicles, roads and the environment [2–4]. It also includes the processing, computing and dissemination of information between entities and systems. These data are used to provide directions for safe driving or eco-routing and offer abundant multimedia and mobile Internet application services. The IoV system consists of three levels: the local that consists of the sensors that the vehicle uses in order to collect information from the surrounding environment, the connection system that uses all means of communication capabilities in order disseminate the information and the cloud services level that provides the vehicle with information needed according to the application.

*Corresponding author. Email: l.maglaras@surrey.ac.uk

Modern vehicular communications include Dedicated Short Range Communications ($DSRC$), based on 802.11p, $WiFi$, and Long Term Evolution (LTE), in order to cope with all kinds of applications (safety, infotainment, routing) and scenarios (urban, suburban, highways) The LTE standard specification not only promises users a truly broadband experience, but also enables mobile network operators to deliver sophisticated services in an effective manner. It has been envisioned to exploit the very existing LTE infrastructure to support vehicular networking applications either through an advanced LTE-enabled OBU or by using smartphones with LTE connectivity. However, the key challenge is to deliver time-constraint data over the $4G/LTE$ connection and to share resources with the mobile users efficiently. Authors in [5] combined the LTE and cloud-based architecture into a unified framework to offset the scalability issues. By locating server closer to the vehicles and multicast/broadcast downlink communication techniques, their proposed framework improves the effectiveness of road safety.

Social Internet of Things ($SIoT$)[6–8] is a new term used to describe a social network of intelligent objects and analogous to Social Networks Services (SNS) for human beings, it introduces the concept of social relationships among objects. Waze, a community-based traffic and navigation application updated in real-time by its users, is a perfect example of the social network of things. The application allows users to update information like road conditions, traffic, and accidents to help people find the best route to get to work, back home, or to the store.

The social aspect of vehicles is examined in this article. The mobility of vehicles, as they travel in a city region, is stored and used in order to create distinct social profiles. These profiles can be used to perform ranking, stable clustering, efficient eco-routing and effective message dissemination in an urban environment. In order to facilitate message exchange between entities the dynamic formation of a multi-hop backbone network is needed. We use the term backbone to identify a virtual chain of vehicles in a vehicular scenario. Each node of the backbone must be connected to previous and next hop of the backbone chain. The backbone formation and management should be determined in a distributed way, by exploiting some characteristics of like the social behavior of vehicles. Stable clusters, e.g. clusters where nodes change their cluster membership less often, can be used as a basis for efficient message dissemination in a high dynamic vehicular environment.

1.1. Contributions

This paper presents a social aspect of vehicular communications and makes the following contributions:

- Puts forward a proposal for a new ranking method of vehicles based on their travel history. Vehicle paths are collected from road side units and are used to rank the road segments and the vehicles in a city area. This metric is used for efficient message dissemination.

- Presents a new clustering method based on vehicle social patterns that improves cluster stability. The proposed $E-SPC$ method takes advantage of the advanced communication capabilities of the vehicles concerned.

- Presents a new dynamic wireless charging method that increases vehicle total range, which is combined with LTE communications and vehicle social patterns for better performance.

- Proposes a distributed intrusion detection mechanism, which can be mounted in vehicles that have a central role in the network.

The rest of this paper is organized as follows: Section 2 describes the communication mechanisms between the vehicles and the cloud. In Section 3 a new ranking metric for vehicles is proposed based on historical data. Section 4 presents the aforementioned social clustering method for vehicles that improves cluster stability. Section 5 shows how cloud computing can increase the total range of electric vehicles. Section 6 discusses security issues and proposes distributed intrusion detection mechanisms and section 7 concludes the article.

2. Communication mechanisms

In order to create the social profile of every vehicle we first split the city into subnetworks and then record the mobility of vehicles in each and finally, use this information to create social profiles for each vehicle. The history of the vehicles is stored on the cloud, and all the calculations needed for the creation of the social profiles are performed off-line. This way, the overhead induced to the vehicle is limited and all the real work is done on the cloud.

2.1. Road network communities - subnetworks

Many approaches focus more on how to partition and manage a network, such that the number of boundary/border nodes for each subnetwork is uniform and minimized, they are approximately of equal size, and so on. We use partitioning based on [9], where each subnetwork forms an isolated part, and the different ones are connected together via intergroup arcs (arcs that are incident to/from boundary nodes and do not belong to any subnetwork). The city is then partitioned into small areas that can be investigated in isolation, which are called subnetworks. Road side units $RSUs$ are assumed to be located at every entry point/exit of each subnetwork with the purpose of collecting driving behavior for every vehicle that leaves it. When the vehicle re-enters the area these historical data are used in order to assign a social number to it.

Figure 1. City is divided in subnetworks. RSUs are located at the entrances/exits of each subnetwork.

$RSUs$ are assumed to be located at fixed locations at the borders of the region of interest. As vehicles move through the network, they record every road segment S_j they traverse in their order of arrival. Every second, each RSU broadcasts a short message to all vehicles in its vicinity, which requests each of these to send their collected set of segments. Upon receipt, the vehicles will create a packet containing the partial path collected as well as other attributes and each vehicle has a unique identifier V_i.

2.2. Vehicle leaving the subnetwork

As vehicle V_i leaves the region of interest and goes into the control range of the intersection, the RSU device near the boundary of the control range impels this vehicle to send information about its trip. This information consists of the collected set of segments, also known as partial path PP_i and travel time T_j, for each road segment j traversed, also known as partial time path PT_i. Upon receipt, the vehicles will create a packet containing the partial time path collected as well as the other attributes, as shown in Figure 2.

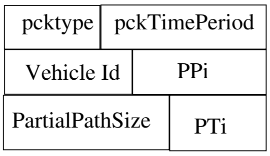

Figure 2. Vehicle packet design (PP_i: partial path, PT_i: partial time path)

Each RSU has a database that contains all the partial paths that the vehicles traverse in the investigated area, which consists of a separate table PPT_{ik} for every vehicle i and for every time period k. This means that for a single vehicle there may be several tables, one for each time period, according to the segmentation of time. On the RSU side, received collected partial paths will be added to their databases according to the nature of the received packet and if it contains a vehicle ID that does not exist in the database, a new table for this will be created. However if the vehicle ID in the packet already exists, the partial path is appended to the existing vehicle table PPT_{ik} and every β seconds, the $RSUs$ can provide each other with the information collected.

The investigation time is segmented into time periods TP. It has been observed [10] that in practice, weekdays and weekends usually exhibit significantly different traffic conditions, whilst at the same having similar congested and congestion-free traffic patterns. Therefore we group the days and treat of these separately. The time periods are pre-dawn: (up until 8am), morning rush-hour (8am to 10am), late morning (10am to noon), early afternoon (noon to 4pm), evening rush-hour (4pm to 7pm), and night time (after 7pm). The paths table PPT_{ij}, shown in Table 1, represents the set of vehicle movement patterns during their trips in the monitored area and as shown below, each vehicle V_i will have a table in this database describing its movement paths for each time period. The table contains all road segments S_j that vehicle V_i traversed when traveling through the subnetwork.

V_{ID}	*Partial Paths*
V_1	$[S_1, S_2, S_3, S_5]$
V_1	$[S_1, S_2, S_4, S_4]$
V_1	$[S_1, S_4, S_3, S_5]$

Table 1. Path table of vehicle i for time period j.

3. Ranking of vehicles - message dissemination

3.1. Data dissemination

Data dissemination generally refers to the process of spreading data or information over distributed wireless networks. From the networking point of view, it requires broadcast capabilities at the link layer that allow a frame to be transmitted to all the vehicles in the radio scope. It also supposes implementation of network and transport mechanisms to disseminate the message across the whole network, which uses one of the two available communication modes. That is, the message will be disseminated in a multi-hop fashion when the vehicle-to-vehicle ($V2V$) communication is enabled and will be broadcast by all the ($RSUs$) when infrastructure-to-vehicle ($V2I - I2V$) communications are used instead. A hybrid version is also possible, whereby $RSUs$ broadcast the messages and, as they do not cover the whole network, some vehicles are selected to forward them to complete the dissemination. These messages can be flooded at a certain number of hops or in a given area (geocasting) depending on the application purposes. In $V2V$ mode, the tasks of a dissemination protocol consist of selecting a pertinent set of vehicles to disseminate the message, and defining retransmission procedures to ensure the entire application requirements regarding reliability, delay, etc.[11]. Modern communication systems that exploit LTE and $DSRC$ communication capabilities are also investigated and developed mostly for safety and traffic management applications (Figure 3).

3.2. Broadcast Storm problem

There is a well-known problem in broadcasting in ad hoc networks, usually referred to as Broadcast Storm, which happens if we use basic flooding, also called blind flooding, to disseminate a packet in the network and works as follows. When a node receives a packet which has to be disseminated in the network, it checks whether it is the first to receive it. If yes, it broadcasts it; otherwise it silently discards it. Since each node forwards the packet, it leads to an important redundancy, which

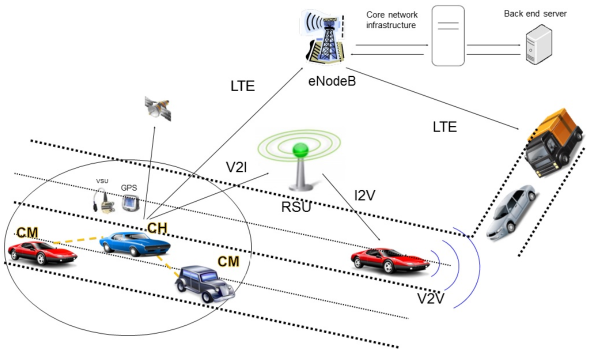

Figure 3. Data dissemination in VANETs

depends on the network density, i.e. a node will receive as many packets as it has neighbors in its radio range. A typical situation in a VANET when the broadcast storm problem occurs is when there is a road accident (Figure 4). When an accident happens in a road segment at a point in time where traffic is intense the road is partially or totally blocked. In such a situation the density of vehicles increases dramatically and a method is necessary for the proper dissemination of safety messages.

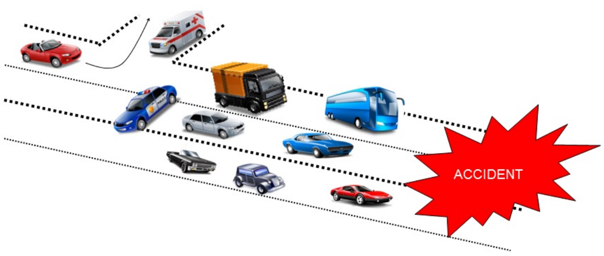

Figure 4. The broadcast storm problem may lead to safety-related service disruption after a road accident

In a VANET, a node may have up to 100 neighbors (the radio range of the IEEE 802.11p may reach up to 1 km and the density of vehicles may reach more than *100* vehicles per kilometre). Since every vehicle sends at least one beacon message every second, basic flooding will lead to *100* receptions per second for each vehicle. Such a scenario will significantly congest the network, causing packet transmissions to face heavy collisions, therefore wasting a lot of bandwidth and CPU resources[11].

Originating from the source node a message will be broadcast through the relay nodes in order to reach the destination or cover the target area. This multi-hop broadcast procedure demands the appropriate selection of relay nodes, which are a subset of surrounding vehicles, in order to ensure that all those in the target area are informed on time. Since in VANETs ack/nack messages are not implemented, a certain level of redundancy, in terms of relay nodes, is required.

An appropriate protocol is required to ensure good dissemination of messages [12, 13]. It is not possible to perform optimal flooding, which minimizes the number of forwarders, because a complete and updated view of the topology is needed. This requires a set of mechanisms which are not necessarily available in every vehicle, i.e. a link sensing mechanism allowing each node to discover its neighborhood, a link state routing protocol, etc. Detecting the most central nodes based on the connection characteristics of all the nodes is important for efficient data delivery in VANETs. The most important issue is to select a forwarding path with the smallest packet-delivery delay and central nodes can create a backbone network which can be used for effective message forwarding. In order to address specific requirements of different applications, such as delay, area coverage etc., knowledge of the topological characteristics of the VANET communication graph is required, where vehicles correspond to vertices and communication links to edges. Vehicles can be clustered into local groups based on these centrality metrics.

3.3. Social message dissemination

In order to rank the vehicles, we propose a proactive ranking of each road segment according to how many vehicles that enter the network are going to traverse it, based on their historic data. For vehicles with no previous historic data the shortest path in terms of distance is assumed to be that preferred. Each vehicle is ranked based on the ranking of the road segments that constitute the path that is going to follow.

In order to calculate the ranking of every road segment, we use the information stored in Table 1. According to this table, we can find the road segments that are going to be highly populated during the next time period and rank them using the algorithm:

Data: Table 1
Result: Ranking of Road Segments
initialization;
while *not at end of Table 1* **do**
    read current;
    if k = *current time period & $S_j \in PPT_{ik}$* **then**
        $R_{jk} = R_{jk} + 1$
    else
        next
    end
end

Algorithm 1: Social ranking of road segments

Using this algorithm, every road has a unique ranking for every time period k and for each vehicle we calculate a ranking based on equation 0.1.

$$R_{V_{ik}} = \frac{\sum_j R_{jk}}{N}, \quad j \in PP_i \tag{0.1}$$

This metric represents the significance of the node in terms of its dissemination capabilities, i.e. the vehicle that is going to follow populated road segments is a better candidate to be selected as a relay node. Routing protocols that rely on employing selected nodes to retransmit a message among the nodes of the network, using the social ranking can be implemented. The selected nodes, which are called multi point relays (MPRs), can effectively disseminate the information avoiding the flooding of messages that cause communication problems among the vehicles.

4. Vehicle clustering

4.1. Cluster based scheme

With a cluster-based scheme, nodes are supposed to be divided into a set of clusters, each being a subset of vehicles forming a convex network. Clusters are supposed to be disjoint, i.e. a node can belong to only one cluster, but in some situations overlapping clusters are created where the nodes that belong to more than one are the gateway nodes. The basic idea is that of grouping network nodes that are in physical proximity, thereby providing the flat network a hierarchical organization, which is smaller in size, and simpler to manage. The subsequent backbone construction uses the induced hierarchy to form a communication infrastructure that is functional in providing desirable properties, such as minimizing communication overhead, choosing data aggregation points, increasing the probability of aggregating redundant data, and so on. A lot of clustering protocols [14–16] have been proposed for ad hoc networks and VANETs.

Generally, a node in a cluster is classified as a head, gateway, or a member. The head, also called cluster head, is a particular node used to build the cluster. There is only being one cluster head in each cluster and it is often at the core of its cluster. Gateways, as mentioned above, are the nodes sharing a link with another cluster and members are the nodes which are neither heads nor gateways. Most of the clustering schemes introduce additional messages which are translated into overhead. However, the clustering-specific messages are exchanged via the control channel (IEEE 802.11p) and this does not affect the dissemination of data.

4.2. Social clustering of vehicles

In order to create stable clusters we use the social behavior of vehicles based on historical data collected from $RSUs$ that are scattered along the borders of each subnetwork of the city. So as to incorporate these data when moving in urban environments every beacon message is allocated one additional byte of information about the social pattern - flow (SN) that the vehicle has. The method is called Sociological Pattern Clustering SPC [17].

The first step in creating a cluster for every vehicle is to identify its neighbors, which is the process whereby a vehicle/node identifies its current neighbors within its transmission range. For a particular vehicle, any other that is within this range is called a neighbor and the neighbor set is always changing since all nodes are moving. Every moving node keeps track of all neighbor ID's as well as their current and past distances. In order to perform clustering using social criteria, SPC maintains two different sets of neighbors. That is, set N_i is the set of all neighbors in range of vehicle V_i and set NS_i is the set of all those that share a common social pattern.

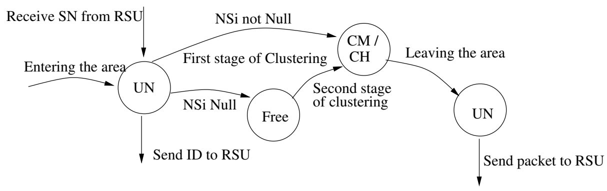

Figure 5. States of a vehicle.

The clustering procedure consists of two stages. In the first stage, clusters are created among vehicles that share common social patterns, after which some clusters will have been formed, but there will also be nodes that could not join any during this phase mainly because they are surrounded by vehicles with different social patterns. At this stage, the set N_i of all neighbors is used and hence, clusters of vehicles with different social patterns are created. Figure 5 represents the different states of a vehicle (undefined, free, member, clusterhead), and the transitions among these when the vehicle enters, moves around or leaves the subnetwork. When the vehicle first enters the subnetwork or leaves it, its state is undefined, UN, since every region is studied in isolation. The SPC method has been proven to be effective in terms of cluster stability and cluster size.

Selection of the clusterhead can affect cluster performance, for it is responsible for controlling the communication inside the cluster, aggregating the information and sending dedicated messages to nearby clusterheads or to a central system. In order to achieve this, among the nodes of a cluster, only those that have dual communication capabilities(both DSRC and LTE) must be elected as clusterheads. In case of no dual interface vehicle, the more stable node of these is elected as a clusterhead according to some microscopic analysis [16]. If more than one vehicle has dual interface capabilities, then it is also the more stable

Data: Cluster members
Result: Clusterhead
initialization;
exists=0;
while *not at end of Table* NS_i **do**
  read current $NS_i(j)$;
  if $NS_i(j)$ *has dual interface* **then**
    exists = 1;
    if NS_ij *more stable* **then**
      NS_ij is elected as a clusterhead
    else
      cluster member
    end
  else
    cluster member
  end
end
if *exists=0* **then**
  i is elected as a clusterhead
else
  cluster member
end

Algorithm 2: Cluster head election algorithm

one that is elected as the clusterhead. The algorithm 2 describes the procedure that runs for every member of the cluster, which is called Enhanced Sociological Pattern clustering $E-SPC$ and is a variation of the original SPC that takes advantage of the advanced communication capabilities of the vehicles. In Figure 6 a cluster created from the $E-SPC$ method with the cluster head algorithm is shown.

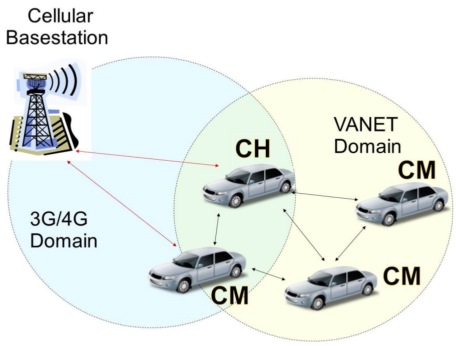

Figure 6. A typical social cluster and the corresponding cluster head of $E-SPC$ method

5. Eco-routing - dynamic charging

5.1. Limited range

With regards to the future transport arena, electric vehicles (EVs) are considered as the likely replacement of the internal combustion engine, especially given the CO_2 reduction and alternative energy perspectives. (EVs) have the potential to reduce carbon emissions, local air pollution and the reliance on imported oil [18]. In Europe, the European commission aims to reduce road transport emissions by *70%* by *2050* [19]. Taking into account the fact that road transport is expected to double by *2050*, passenger cars need to reduce their emissions significantly. Advanced internal combustion engine (ICE) technologies are expected to enable emissions reduction, but are not expected to meet long term targets. (EVs), especially plug-in ones ($PEVS$), are penetrating the market and they are currently counted as zero emissions vehicles. Apart from the additional cost of their lithium-ion battery pack that makes them more expensive than conventional vehicles, there are also some other factors that discourage drivers from switching to an EV. For instance, battery powered ones have a limited driving distance [20] and hence, the current lack of charging infrastructure as well as the total time needed to recharge such a vehicle add to their lack of desirability.

In order to surmount this problem, industries and research institutions around the world have proposed numerous solutions. These vary from stationary stations that are scattered across the road network in central positions [21–23], to dynamic wireless charging methods that take advantage of mobility of nodes [24, 25] and eco-routing algorithms that run in isolation in every vehicle or in a central way for a fleet of vehicles [26–28]. Dynamic wireless charging is gaining more ground, since it enables power exchange between the vehicle and the grid whilst the former is moving. Installed infrastructure can be utilized very effectively, because many vehicles use the same road segments that are "equipped" with dynamic charging capabilities. Dynamic charging can take place in a parking lot, at a bus stop during passenger disembarkation, along a highway or near traffic lights.

5.2. Mobile energy disseminators

Similar to information dissemination, special nodes, like buses (trucks), can act as energy sources for EVs that need charging, in order to increase travel time. These vehicles, from now on called mobile energy disseminators ($MEDs$), use electric plug in connection or IPT in order to refill starving EVs. The vehicle requiring electric charge approaches the appropriate truck, after a preceding agreement, from the rear or the front end depending on the vehicle construction. The procedure provides vehicle charging by an electric plug in connection (or process), or by electromagnetic induction with the use of Tesla coils. By using cooperative mechanisms, based on dedicated short-range communication ($DSRC$) capabilities of vehicles or long term evolution (LTE) technology, vehicles search for the $MEDs$ in range and arrange a charging appointment while moving [25].

For the LTE system (see Figure 7), we assume that vehicles are equipped with The Evolved Universal Terrestrial Radio Access Network ($EUTRAN$) interface, which enables them to communicate with the eNB so as to access the core components of the LTE. LTE Evolved Node B (eNB) base station transceivers are deployed alongside the road network in order to cover the area. Each bus communicates to the LTE the scheduled trip that is going to be followed, the available charging capability, the energy value and charging availability. All vehicles are assumed to be equipped with GPS.

Each EV that needs energy:

1. Checks whether MED is on his route or not according to their social patterns
2. Checks whether the CC level is high enough so as to cover its energy needs
3. Checks whether the MED is already fully booked
4. Books a charging place
5. Drives in front or behind the bus for the determined time in order to recharge

The architecture of the proposed mobile energy dissemination procedure is demonstrated in Figure 7. The benefits of such an approach are threefold: first, it utilizes existing cellular infrastructure. Second, the 802.11$pnetwork$ overhead introduced by frequent communication between EVs and $MEDs$ is offloaded. Third, information is more up to date than that received through IVC, where many intermediate relay nodes may be needed in order to disseminate data effectively. However, vehicles are required to have two types of network interface cards and packets that pass through the LTE core potentially experience more delay.

Optimal route selection overcomes a common problem that of when all vehicles prefer the same paths, leading to over congestion. Optimal routing of vehicles that use this new technology can be formulated as a modified shortest-path problem, where the weights of the road segments may vary over time, according to the existence or not of a MED traveling on the road segment [29]. The use of LTE technology helps the vehicles communicate with a MED that could not be reached with the use of $DSCR$ technology. Also, the social patterns of the vehicles can be exploited from the system so as to decrease rerouting of vehicles, since only nodes that share common habits may be favored from the system to exchange energy.

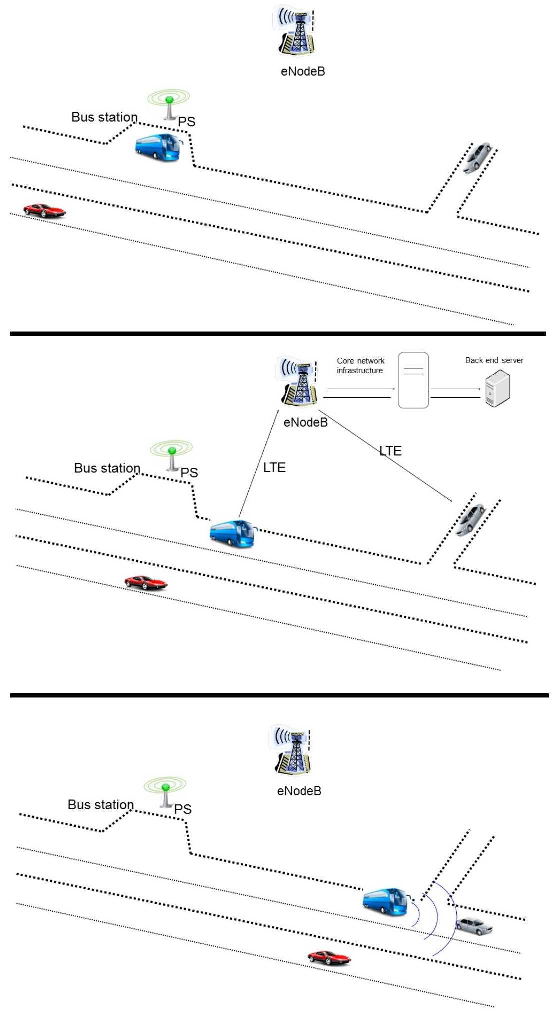

Figure 7. Application example of a Mobile Energy Disseminator: A. Contactless charging is used to deliver charging to a bus B. There is LTE communication between MED and EV C. The electric vehicle recharges from the bus with inductive power transfer (IPT)

6. Security & privacy issues

6.1. Intrusion detection

So far, the research on Intrusion Detection Systems ($IDSs$) has been targeting the CAN protocol [30]. Both specification-based and anomaly-based detection methods have been proposed. Hoppe et al. [31] has demonstrated an anomaly-based IDS for the CAN protocol, which detects deviations on the number of transmitted messages by considering the rate of how often specific messages are transmitted on the CAN bus, and comparing this to what is deemed to be normal. When the anti-theft alarm is activated, the system sends messages to the lights of the vehicle to turn them on and off, so that they are flashing. Furthermore, several approaches to introducing Intrusion Detection System

(IDS) into vehicles have been suggested. Regarding which, both specification-based [32] and anomaly-based treatments [33, 34] have been investigated. Moreover, an attempt to deflect attacks using honeypots has been described in [35].

In the new interconnected world we need to secure the IP based Ethernet Channel using both specification-based and anomaly-based approaches. In the next subsection we present our integrated intrusion detection mechanism [36] and how it could be used in a Vanet environment by using the social characteristics of the vehicles.

6.2. OCSVM based intrusion detection system

The main purpose of the IT-OCSVM detection mechanism is to perform anomaly detection in a time-efficient way, with good accuracy and low overhead, within a temporal window. In order to achieve the aforementioned goals several operation stages need to be carried out: Pre-processing of raw input data, feature selection, creation of detection modules, fusion of initial alarms and the reporting of an alarm to the system. Pre-processing is used so as to transform data of incoming packets to a convenient format for the classification modules. After this step, the most appropriate features are selected and the intrusion detection modules created, which produce initial alarms indicating a variation in network traffic from what is normal. Since the initial alarms may be too many, fusion methods that include ensemble, aggregation and k-means clustering are used. The final alarms that may be produced are communicated from the system to the management authority in order to report the attack and to decide upon the counter measures to be taken.

The intrusion detection mechanism (see Figure 8) can run in the cloud by analyzing the network traffic that is sent both from the RSUs that are scattered along the road network and from the vehicles that have LTE capabilities. A lighter version (distributed detection agents) can operate in some central vehicles by analyzing the packets sent in the vehicles neighborhood, and these central vehicles can be chosen by using the $E-SPC$ method presented in Section 4. Each vehicle that detects a possible attacker may communicate this information to the system through a dedicated message. The central system gathers the information received from the distributed agents and takes final decisions about the severity of the alarm.

6.3. Privacy

Privacy preservation is critical for vehicles and in this context is achieved when two related goals are satisfied: untraceability and unlinkability [37–39]. The first property refers to a vehicle's actions not being able to be traced and the second, that it must be impossible

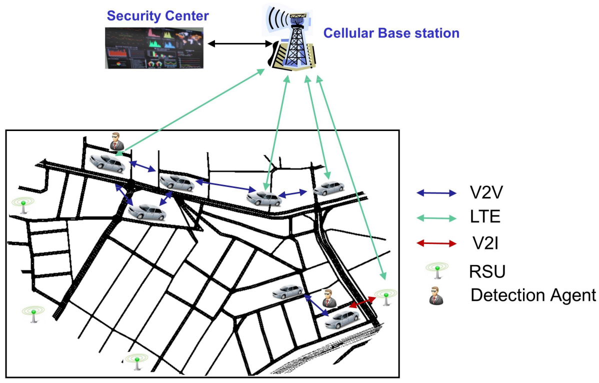

Figure 8. Intrusion detection mechanism

for an unauthorized entity to link its identity with that of its driver/owner. On the other hand, no traffic regulation or congestion avoidance can be achieved if this privacy protection is not removed. That is, access to the data concerning owner identity for a given vehicle and the path followed along a period of time are crucial for building its social profile. Therefore, security mechanisms should prevent unauthorized disclosures of information, while on the same time allow an appropriate amount of data to be fed to the applications in order to work properly [40].

7. Conclusions

In this article the social aspect of vehicular communications is investigated. The mobility of vehicles is tracked and stored in a cloud based system and social patterns for every vehicle are created. These patterns are used in order to rank road segments and vehicles dynamically. Ranking of vehicles can be used in order to perform efficient message dissemination by selecting the nodes that follow populated roads so as to alleviate the broadcast storm problem. In order to cope with the interference caused by flooding of messages clustering of vehicles is also used and the social patterns of vehicles are employed to ensure the creation of stable clusters. Combined communication capabilities can also facilitate eco-routing and dynamic charging of electric vehicles. In addition, the social patterns of the vehicles can be exploited from a dynamic wireless charging system so as to decrease rerouting of vehicles, since only nodes that share common habits may be favored from the system to exchange energy.

In order to secure vehicular communications, we propose a hybrid central and distributed system that is based on machine learning techniques. The system is based on an intrusion detection mechanism that can achieve high accuracy and a low false alarm rate. Except from a central detection system that operates on the cloud, distributed agents that run on central vehicles collect and analyze network traffic and report malicious activity to the security center in real time.

References

[1] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): A vision, architectural elements, and future directions, Future Generation Computer Systems 29 (7) (2013) 1645–1660.
[2] N. Lu, N. Cheng, N. Zhang, X. Shen, J. Mark, Connected vehicles: Solutions and challenges, Internet of Things Journal, IEEE 1 (4) (2014) 289–299.
[3] M. Gerla, E.-K. Lee, G. Pau, U. Lee, Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds, Internet of Things (WF-IoT), 2014 IEEE World Forum on.
[4] N. Liu, Internet of vehicles: Your next connection, in: WinWin, huawei, 2011, pp. 241–246.
[5] S. Kato, M. Hiltunen, K. Joshi, R. Schlichting, Enabling vehicular safety applications over lte networks, in: Connected Vehicles and Expo (ICCVE), 2013 International Conference on, IEEE, 2013, pp. 747–752.
[6] K. M. Alam, M. Saini, A. El Saddik, tnote: A social network of vehicles under internet of things, in: Internet of Vehicles–Technologies and Services, Springer, 2014, pp. 227–236.
[7] L. Atzori, A. Iera, G. Morabito, M. Nitti, The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization, Computer Networks 56 (16) (2012) 3594–3608.
[8] L. Atzori, A. Iera, G. Morabito, Siot: Giving a social structure to the internet of things, Communications Letters, IEEE 15 (11) (2011) 1193–1195.
[9] Q. Song, X. Wang, Efficient routing on large road networks using hierarchical communities, IEEE Transactions on Intelligent Transportation Systems 12 (1) (2011) 132–140.
[10] R. Simmons, B. Browning, Z. Yilu, V. Sadekar, Learning to predict driver route and destination intent, in: Proceedings of the IEEE Intelligent Transportation Systems Conference (ITSC), 2006.
[11] R. Naja, Wireless vehicular networks for car collision avoidance, in: Springer 2013, 2013.
[12] M. Chitra, S. S. Sathya, Efficient broadcasting mechanisms for data dissemination in vehicular ad hoc networks, International Journal of Mobile Network Communications & Telematics (IJMNCT) 3 (03) (2013) 47–63.
[13] R. Kumar, M. Dave, A review of various vanet data dissemination protocols, International Journal of u-and e-Services, Science and Technology 5 (2012) 27–44.
[14] M. Ni, Z. Zhong, D. Zhao, MPBC: A mobility prediction-based clustering scheme for ad hoc networks, IEEE Transactions on Vehicular Technology 60 (9) (2011) 4549–4559.
[15] E. Sakhaeee, A. Jamalipour, Stable clustering and communications in pseudolinear highly mobile ad hoc networks, IEEE Transactions on Vehicular Technology 57 (6) (2008) 3769–3777.
[16] L. A. Maglaras, D. Katsaros, Distributed clustering in vehicular networks, in: Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2012, pp. 593–599.
[17] L. A. Maglaras, D. Katsaros, Social clustering of vehicles based on semi-markov processes, IEEE Transactions on Vehicular Technologydoi:10.1109/TVT.2015.2394367.
[18] T. R. Hawkins, B. Singh, G. Majeau-Bettez, A. H. Strm-man, Comparative environmental life cycle assessment of conventional and electric vehicles, Journal of Industrial Ecology 17 (1).
[19] H. de Wilde, P. Kroon, Policy options to reduce passenger cars co2 emissions after 2020.
[20] S. Lukic, Z. Pantic, Cutting the cord: Static and dynamic inductive wireless charging of electric vehicles, in: Electrification Magazine, IEEE 2013, vol. 1, no. 1. pp. 57-64.
[21] N. Machiels, N. Leemput, F. Geth, J. Van Roy, J. Buscher, J. Driesen, Design criteria for electric vehicle fast charge infrastructure based on flemish mobility behavior.
[22] G. Putrus, P. Suwanapingkarl, D. Johnston, E. Bentley, M. Narayana, Impact of electric vehicles on power distribution networks, in: Vehicle Power and Propulsion Conference, 2009. VPPC '09. IEEE, 2009.
[23] A. R. Mario, A. A. Fadi, M. Gagnaire, Y. Lascaux, Telewatt: An innovative electric vehicle charging infrastructure over public lighting systems, in: Proceedings of the 2nd International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, USA, December, 2013.
[24] G. Jung, B. Song, S. Shin, S. Lee, J. Shin, Y. Kim, C. Lee, S. Jung, Wireless charging system for on-line electric bus(oleb) with series-connected road-embedded segment, in: Environment and Electrical Engineering (EEEIC), 2013 12th International Conference on, 2013.
[25] L. A. Maglaras, F. V. Topalis, A. L. Maglaras, Cooperative approaches for dymanic wireless charging of electric vehicles in a smart city, in: Energy Conference (ENERGYCON), 2014 IEEE International, 2014, pp. 1365–1369. doi:10.1109/ENERGYCON.2014.6850600.
[26] K. Boriboonsomsin, M. J. Barth, W. Zhu, A. Vu, Eco-routing navigation system based on multisource historical and real-time traffic information.
[27] L. A. Maglaras, P. Basaras, D. Katsaros, Exploiting vehicular communications for reducing co2 emissions in urban environments, in: in proceedings of the IEEE International Conference on Connected Vehicles (ICCVE 2013), Las Vegas, USA, December 2-6, 2013.
[28] L. Zi-fa, Z. Wei, J. Xing, L. Ke, Optimal planning of charging station for electric vehicle based on particle swarm optimization, in: Innovative Smart Grid Technologies - Asia (ISGT Asia), 2012.
[29] L. A. Maglaras, J. Jiang, F. V. Topalis, A. L. Maglaras, Mobile energy disseminators increase electrical vehicles range in smart city, in: Hybrid and Electric Vehicle Conference, IET, 2014.
[30] P. Kleberger, T. Olovsson, E. Jonsson, Security aspects of the in-vehicle network in the connected car, in: Intelligent Vehicles Symposium (IV), 2011 IEEE, IEEE, 2011, pp. 528–533.

[31] T. Hoppe, S. Kiltz, J. Dittmann, Applying intrusion detection to automotive it-early insights and remaining challenges, Journal of Information Assurance and Security (JIAS) 4 (6) (2009) 226–235.

[32] U. E. Larson, D. K. Nilsson, E. Jonsson, An approach to specification-based attack detection for in-vehicle networks, in: Intelligent Vehicles Symposium, 2008 IEEE, IEEE, 2008, pp. 220–225.

[33] T. Hoppe, S. Kiltz, J. Dittmann, Adaptive dynamic reaction to automotive it security incidents using multimedia car environment, in: Information Assurance and Security, 2008. ISIAS'08. Fourth International Conference on, IEEE, 2008, pp. 295–298.

[34] M. Muter, A. Groll, F. C. Freiling, A structured approach to anomaly detection for in-vehicle networks, in: Information Assurance and Security (IAS), 2010 Sixth International Conference on, IEEE, 2010, pp. 92–98.

[35] V. Verendel, D. K. Nilsson, U. E. Larson, E. Jonsson, An approach to using honeypots in in-vehicle networks, in: Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th, IEEE, 2008, pp. 1–5.

[36] L. A. Maglaras, J. Jiang, T. J. Cruz, Integrated ocsvm mechanism for intrusion detection in scada systems, Electronics Letters 50 (2014) 1935–1936(1).

[37] M. Gerlach, VaNeSe – An approach to VANET security, in: Proceedings of the International Workshop on Vehicle-to-Vehicle Communications (V2VCOM), 2005.

[38] M. Whaiduzzaman, M. Sookhak, A. Gani, R. Buyya, A survey on vehicular cloud computing, Journal of Network and Computer Applications 40 (2014) 325–344.

[39] G. Yan, S. Olariu, M. C. Weigle, Providing {VANET} security through active position detection, Computer Communications 31 (12) (2008) 2883 – 2897, mobility Protocols for ITS/VANET. doi:http://dx.doi.org/10.1016/j.comcom.2008.01.009.

[40] J. M. De Fuentes, A. I. Gonzalez-Tablas, A. Ribagorda, Overview of security issues in vehicular ad-hoc networks, in: Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, 2011.