can then build a valid IPv6 address out of the included IPv6 prefix, following the standard SLAAC mechanism, i.e., the host generates an address by joining the prefix received from the RA and the network identifier derived by its MAC address.

The link-local multicast capability emulation is achieved by relying on the geo-multicast/geo-broadcast capabilities provided by the ETSI GN layer. In particular, in order to be link-local multicast capable, an IP link must provide symmetric reachability [3], which is normally not accomplished by virtual links spanning multiple physical links due to the lack of reference boundaries. Link-local multicast packets are forwarded with geographical knowledge, so that a node processes a packet only if it was addressed to the area where the node is located. The geographic scoping provides non-variable virtual link boundaries which enable symmetric reachability. For RAs, this means that RAs must be delivered to – and only to – the nodes that are part of the same IPv6 link, nodes that are actually connected via multiple wireless hops. If a multi-hop path exists, all the nodes within the area will receive a copy of the RA, and the IPv6 instance running above the geo-networking will process the message as if the node was directly connected to the access router that issued the message.

It is assumed that MAC addresses (or a different identifier that can be used for IPv6 address generation purposes) of vehicles are unique, at least within macro-regions where vehicles are sold and can potentially communicate with each other (e.g., a continent). This property in fact is highly desirable for security and liability reasons, as it would allow (i) forensic teams to rely on vehicular communications to reconstruct accident scenes or other critical situations and, (ii) to detect malicious nodes and reduce considerably the effects of network attacks. Despite uniqueness of identifiers, privacy of users can be protected by equipping vehicles with sets of unique identifiers to be used for limited intervals as pseudonyms [13]. These identifiers could be assigned by authorities and, when coupled with the usage of digital certificates and cryptographic protection [14], this mechanism can accomplish support for liability as well as privacy protection from malicious users (commonly referred to as revocable privacy). Assuming that the IPv6 prefix announced by the RSU is exclusively assigned to this area, the address uniqueness is verified, and therefore no Duplicate Address Detection (DAD) mechanism is required. Note that the proposed solution could be applied to multiple RSUs acting as bridges connected to one single Access Router. This might be a good deployment choice in scenarios where single-hop connectivity to the infrastructure is preferred while it is also required to reduce the number of IPv6 address changes (e.g., city environment).

A technique that maximizes the benefits of ETSI SLAAC consists in shaping the GVL areas assigned to the RSU in a adjacent and logically non-overlapping fashion, as depicted in Figure 3. By doing so, the following key advantages are obtained: (i) unequivocal gateway selection is achieved with the infrastructure having full control on it\(^8\), as only one RSU is assigned per geographical area; (ii) a network partitioning is obtained that supports movement detection procedures of IPv6 mobility and also allows for location-based services. In particular, a vehicle moving across regions served by different Access Routers experiences a sharp sub-net change, without traversing gray areas where Router Advertisements are received from multiple access points (potentially leading to ping-pong effects).

Before characterizing and analyzing the performance of the ETSI SLAAC solution, we next analyze under which conditions it is realistically feasible to support IP unicast multi-hop communications in a vehicular environment.

### 3 Effectiveness of Vehicular Multi-hop Communications

Vehicular networks using short-range wireless technologies, such as IEEE 802.11-based ones, rely on multi-hop communications to extend the effective coverage of the RSUs deployed on the roadside. One of the main challenges that VANETs pose is the minimum degree of technology penetration that is needed in order to ensure that there is enough density of communication-enabled vehicles to support multi-hop connectivity between the intended peers (e.g., for the case of Internet communications, between the vehicle and the RSU). This problem becomes even more problematic during the time of the day when roads are less busy. In these situations, vehicular networks need to be more mesh-like in order to be able to create multi-hop paths for IPv6 communications. An example of this is shown in Figure 3, where the geographical area is divided into non-overlapping and adjacent GVL areas.

\(^8\) More precisely, in this solution gateway selection is performed by the infrastructure itself and not by the nodes as in many MANET approaches.