NDN, Technical Report NDN-0072. http://named-data.net/techreports.html
Revision 2: September 4, 2022

Names to Rule Them All: Unifying Vehicular Networking via Named Secured Data

Tianyuan Yu
UCLA
tianyuan@cs.ucla.edu

Zhiyi Zhang
UCLA
zhiyi@cs.ucla.edu

Eric Newberry
UCLA
enewberry@cs.ucla.edu

Alexander Afanasyev
Florida International University
aa@cs.fiu.edu

Giovanni Pau
University of Bologna - DISI and
UCLA Computer Science Dept.
gpau@cs.ucla.edu

Lan Wang
University of Memphis
lanwang@memphis.edu

Lixia Zhang
UCLA
lixia@cs.ucla.edu

ABSTRACT

Over the last few decades, mobile networking technologies have advanced by leaps and bounds, especially in terms of wireless speeds and mobile device capabilities. Yet advanced mobility support for peer-to-peer networking with ad-hoc encounters, seamless integration with infrastructure, and in particular the ability to secure ad hoc mobile communication is yet to arrive. Today's commonly-deployed mobile solutions rely heavily on cloud services over cellular connectivity, even when the communicating mobile entities are in close proximity to each other. Vehicular networking is an exemplifying use case of peer-to-peer networking with ad-hoc encounters, which also desires both strong security and seamless integration with infrastructure networks. We take this use case to motivate a new abstraction of networking, via exchanging semantically named and secured data instead of pushing packets to numeric IP addresses. We illustrate how this new abstraction can effectively support vehicular networking, unify mobile ad-hoc and infrastructure communications by the same network protocol, and build security support into all communications. We also illustrate how this new direction of networking can keep local communications local and support the diverse set of today's vehicular applications, with a potential to support those that are yet to come.

1 INTRODUCTION

Computing and communication technologies have advanced rapidly, giving rise to a proliferation of deployed mobile devices ranging from smart phones to smart vehicles. However, the basic approach to mobility support has not changed significantly either to meet the new communication demands, or to fully utilize the ever increasing computing and storage resources on mobile devices. Many proposed solutions explored diverse directions independently, without converging toward a shared vision.

Given the ever increasing importance that mobile devices play in society, we believe that it is imperative *now* to develop a vision of where we *wish to see* mobile computing in 10 years. In this paper, we first use a specific vehicular networking use case (§2) to identify the challenges encountered in vehicular application development. Next, we offer a new perspective on existing solutions in vehicular networking. In particular, we note the trend from multiple existing works that have started moving away from IP's *node-centric* communication model and moving towards a *data-centric* model (§3). Further, we explore the solution space with a focus on the data-centric approach (§4), by first offering a brief overview of the Named Data Networking (NDN) design [44], then explaining how NDN can provide both the essential framework and the basic building blocks to overcome the identified challenges, enabling a new direction for future mobile networking.

Our basic goal in this paper is to articulate a vision for future mobile networking based on first principles without being constrained by the current state of art. The first principles we consider are as follows:

(1) security is of utmost importance when communication leverages ad hoc encounters, therefore it must be designed into an ad hoc mobile network architecture;
(2) the architecture must support scalability and resiliency, and accommodate heterogeneous technologies at lower layers; and
(3) technology will continue to advance over time, likely at an accelerated speed, and therefore designs for the

future should fully utilize this anticipated advancement.

Rather than conducting a quantitative evaluation of a system that works in a specific setting, this paper provides an overview of NDN-based vehicular networking, which follows the above principles, focusing on several design aspects, including naming, forwarding strategy, link adaptation layer design, and security. We conclude the paper by taking a long, hard look at both today's state of affairs and the path that took us here, and by identifying new tasks in front of us in order to move mobile networking toward a data-centric future (§5).

2 VEHICULAR NETWORKING: A CASE STUDY

In this section, we describe two typical safety application cases in vehicular networking.

By communicating with roadside units (RSUs), smartphones, traffic support infrastructure (e.g., smart traffic lights), as well as nearby vehicles, each vehicle can obtain detailed information about its surrounding to determine the best course of action to take from moment to moment, improving both safety and efficiency of road travel. We first introduce vehicular communication at a traffic intersection as a driving case to identify the required functional support in vehicular networking above the physical and MAC layers. Our objective is to identify the challenges in realizing an ideal solution that offers the most information support for every vehicle.

The first scenario is shown in Figure 1, where the leftmost red car is planning to make a left turn at the upcoming intersection. It may need to adjust its trajectory and speed, based on the presence of pedestrians or vehicles on its planned path; however, its current position does not provide a complete view of the intersection. The cars and the RSUs located near the intersection could provide the desired information to the red car about the presence of a pedestrian over short-range wireless links (such as DSRC [23]). Another option for detecting the pedestrian could be through cellular device-to-device communication between the red car and the pedestrian's phone, for example over LTE D2D [28].

The second scenario is shown in Figure 2, where a collision has occurred in the intersection. To avoid traffic congestion, the information about this collision should be disseminated immediately to all the vehicles within the vicinity – nearby vehicles heading toward the intersection can be notified through either V2V or V2I communication, so that they may turn around instead of getting piled up before the intersection, a situation that is all too common today. Furthermore, given that rescue and cleaning operations after a collision may take some time, the information of this collision event should also be made available to vehicles further away, so that they can take it into account in their route selection. This can be assisted by cloud services, which may collect information from the RSU at the intersection, or from vehicles over cellular connections.

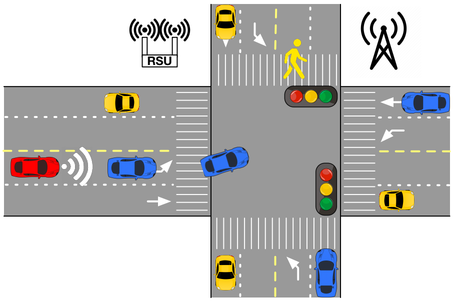


Figure 1: Pedestrian in the Intersection

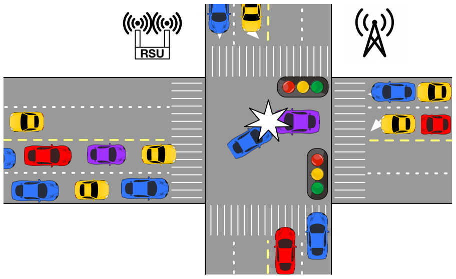


Figure 2: Collision in the Intersection

In the first scenario, the event data producers and receivers are within a localized scope; it is largely the case for the second scenario as well except the notifications for remote vehicles. Currently, all the communications are realized by either a single-hop wireless broadcast at link layer, or otherwise by establishing connections to remote relay points (e.g., cloud). We view such realizations as the artifact of today's TCP/IP protocol stack, which makes it easy to communicate with cloud servers but difficult to communicate with nearby vehicles.

3 A PERSPECTIVE ON PREVIOUS WORKS

In this section, we present our perspective on the existing results in vehicular networking that attempt to provide solutions to aforementioned scenarios.

3.1 Communication Model

This section provides a categorization of recent standards and research efforts based on their abstraction of network packet delivery model. Packet delivery can be based on naive hop-by-hop broadcast, or network connectivity identifiers which are independent from the data being forwarded, or application layer data identifiers. For example, IP addresses indicate topological location of nodes, but do not contain information relevant to vehicular application, such as geolocations.

Information dissemination by broadcast. In order to disseminate data to vehicles and drivers within the vicinity, many existing vehicular systems [7–9, 13, 18, 31, 38] adopt a data broadcast model. When a receiver obtains data, it then determines whether the information is, or is not, relevant, and may rebroadcast data based on application layer's decisions. This blind broadcast approach inevitably leads to nodes receiving duplicate and irrelevant packets. For example, in [18], each vehicle broadcasts sensed traffic information (e.g., the time it took to drive between two points). However, such information may not be relevant to all other vehicles. Similarly, in [7], in order to disseminate road traffic congestion information, vehicles broadcast alert messages periodically. A major concern with such blind broadcast by any nodes is its inability to utilize the limited capacity of network channels in the best way possible, for example handling the most urgent messages with highest priority.

Packet delivery based on network connectivity identifiers. A number of works [17, 35, 39] developed vehicular communication solutions based on existing TCP/IP address-based point-to-point packet delivery, together with the routing mechanisms adopted from wired networks. In addition, many standards [1–3, 15, 16] support the use of TCP/IP protocols for communication between vehicles and the Internet infrastructure. Although TCP/IP is mature for stationary infrastructure networks, it takes significant effort to handle the unstable connectivity, addressing, and network handover issues in vehicular networks, due to the fundamental discrepancy between TCP/IP's point-to-point delivery using IP addresses and the highly dynamic connectivity in mobile vehicular networks.

For example, IEEE 1609.3 (i,e., WAVE) [1] specifies an IPv6 addressing scheme, service primitives, and mechanisms for RSUs and vehicles to establish point-to-point data delivery relationships. It categorizes nodes into stationary devices (i.e., infrastructure) and mobile devices (i.e., vehicles). The infrastructure's IP addresses are provisioned by network administrators according to operating policies, while individual vehicles learn the IP prefix of current IP network by listening to the routing advertisement from the infrastructure nodes (e.g., RSUs). Afterwards, vehicles can derive their own IPv6 addresses by means of stateless configuration, by concatenating the obtained infrastructure's IPv6 prefix with their own MAC address.

However, exposing one's MAC address raises privacy concerns. Later IPv6 standard [19] mitigates this issue by generating randomized identifiers to obtain temporary addresses. WAVE also supports device readdressing to provide pseudonymity. Therefore, a WAVE vehicle's MAC address may be randomly generated and change at any moment, leading to the issue of duplicate address detection in highly mobile scenarios. As soon as the vehicle roams to another area covered by a different RSU, the previous detection result becomes invalidated. Later works [10] seek to address them by introducing additional mechanisms in the handover process.

Packet delivery based on geo-identifiers. Recognizing the importance of utilizing data semantics to facilitate vehicular communication, a number of efforts proposed geographic location-based routing and forwarding [5, 6, 11, 22, 26, 33]. For example, geocasting protocols [25, 30] forward packets based upon the destination "Zone of Relevance" (ZOR), which can be viewed as a geographic location. This provides new capabilities to applications and greatly reduces the complexity of the system. ROVER [24] takes ZORs a step further to bind application identifiers to forwarding, by defining a message as the triplet of application, payload, and receiver ZOR. Data is forwarded to all nodes within the ZOR based on the information identifiers. Thereby the forwarding decisions, instead involving only ZOR, also consider applications' different interests for data. Packet delivery based on geo-identifiers moves away from traditional node-centric communication, as the forwarding decisions are no longer determined by connectivity information.

3.2 Securing Vehicular Communications

Security and privacy have been investigated in prior vehicular networking standards and research efforts [36]. We split existing work into two categories based on what security being addressed. The first category secures network channels that transport data, i.e., a TCP connection – in these systems, data is not secured after it leaves the channel. The second category secures data directly, so security properties stay with the data itself.

Securing channels. A few system solutions of vehicular security rely on secured channels, such as TLS [34]. For example, IEEE 1609 (i.e., WAVE) standard [2] enables vehicles to establish TLS sessions with the infrastructure to obtain certificates, and utilize a Web API to securely encapsulate data. However, due to the highly mobility of vehicles, connections in vehicular networks are unstable, making connection-oriented security ineffective.

Securing data. To overcome the limitations of secured channels, data-centric security solutions [4, 21, 29, 37, 41, 45] have been proposed to provide data security independent of underlying connections in vehicular environments. They also ensure vehicle/driver privacy by hiding identifying information by various mechanisms, including anonymity, pseudonyms, and group/ring signature schemes. For example, IBRS [29] integrates a digital signature into each application data message, so that the receiver can verify that the data was signed by a valid vehicle in the vicinity of itself. This authenticity information uses ring signatures to hide vehicle identities.

As demonstrated above, securing data provides many benefits over securing channels, given the dynamic nature of connections and topologies in vehicular environments.

Because securing data requires individual vehicles to verify the identity of packet sender, trust models are needed to specify the trust relations among real world entities such as RSUs and vehicles. Therefore, besides using per message signature, some solutions also introduce the trust models to vehicular networking. For example, ETSI ITS [14] proposes a trust hierarchy which consists of three major components – manufacturers, enrollment authorities, and authorization authorities. In this framework, manufacturers assign unique identities (i.e. byte strings) to each vehicle/RSU. Enrollment authorities will then issue credentials for vehicles that they trust to function properly, while authorization authorities issue credentials to vehicles when they require some specific permissions (e.g., broadcasting certain type of messages). Meanwhile, WAVE uses the Security Credential Management System (SCMS) [40] trust hierarchy developed by U.S. Department of Transportation (DoT). In SCMS, enrollment CAs issue certificates to vehicles and RSUs to certify that they are trusted actors in the system. Vehicles can then use these certificates to obtain pseudonyms from pseudonym CAs. On behalf on the On-boarding Equipment (OBE) on vehicles, a separate Device Configuration Manager (DCM) securely communicate with CAs by mutually authenticated TLS connection, and request certificate enrollment. Then human operators use DCM to manually transfer the enrollment certificate and private keys to OBE in a physically secure location (e.g., a secure room where physical cable connections can be visually inspected).

3.3 Remaining Challenges

From the previous works described in the above, we can identify the following three remaining challenges that need to be addressed in order to provide the most information to all relevant vehicles.

Unstable Wireless Connectivity. Both scenarios in Section 2 suggest that multiple paths may exist among the nearby vehicles, roadside infrastructure, and pedestrians' smartphones. At the same time, due to the high mobility, such wireless connectivity can be intermittent and highly unstable. Ideally, one would wish to make the best use of *any* and *all* available wireless connectivity options, however short-lived they may be.

Unfortunately, from the functions provided, this wish is far from the existing Internet protocol stack, which was initially developed to run over stable network infrastructures. For example, routing protocols take time to adapt to connectivity changes, and most of them do not support multi-path forwarding. In addition, packet losses require end-to-end retransmission. Many efforts have attempted to modify *individual* parts of the existing protocol stack to meet some of the mobile networking needs, e.g., MANET routing protocols, epidemic data dissemination, and TCP proxies for performance improvement. However, these piecemeal solutions are developed in isolation, and none of these efforts considered an overall framework that can go beyond addressing a specific problem.

Inefficient Information Dissemination under Dynamic Network Topology. The ultimate goal of vehicular networking is to get the needed information to applications, regardless of the underlying connectivity, be it ad hoc wireless or a cellular channel. For example, the red car in Figure 1 needs to get the information about pedestrian presence at that intersection. The information may be delivered via any of the multiple paths, ideally through means that can maximize the delivery success and minimize the delay, and the information should be authentic.

However, with the existing TCP/IP protocol stack, the red car must first learn the IP address of some node that can provide information about the concerned intersection. Since the red car cannot know a priori the IP addresses of its surrounding vehicles or RSUs, existing vehicular applications generally rely on cellular connectivity to communicate with cloud servers. In this example, however, cloud-based services may be infeasible due to the delay constraints. One proposed solution is to have all the devices proactively flood all the information regarding the intersection to all nearby devices, which may also forward the information further. This brute-force solution, although simple, may seriously jam the wireless channel depending on the number of cars and other devices at the intersection. Uncoordinated flooding will likely result in relevant information being lost due to congestion caused by irrelevant information.

Lack of Usable Security Solutions in Ad Hoc Mobile Communication. Any information exchange, especially for critical applications such as road safety, needs security protection against modification (to ensure data integrity) and false injection (to ensure data authenticity). In addition, the identities of individual drivers/vehicles must be protected to assure user privacy.

Although today's Internet has seemingly mature security solutions for cloud-based applications, those solutions rely on certificate authorities to authenticate cloud servers, and depend on encrypted stable TCP connections. This set of solutions work well over stable infrastructure connections, but are ill-fitted to mobile networking, where communication occur during ad hoc encounters via unstable wireless connectivities.

3.4 Limitations of IP in Ad Hoc Mobile Networking

Although the discussion in this section focuses on two specific examples in vehicular networking, we believe that the three identified challenges are applicable to ad hoc mobile networking in general. Unstable wireless connectivity is caused by the mobility of communicating devices, vehicles or not. Information dissemination is inefficient because the existing IP protocol is designed for point-to-point delivery. Furthermore, the MANET research efforts have largely focused on either ad hoc routing protocol development or brute-force data delivery via hop-by-hop multicast of UDP packets, leaving the security challenges largely unaddressed.

IP's point-to-point communication model with numeric addresses limit the solution space of the second challenge. Point-to-point communications make information dissemination inefficient, while numeric IP addresses do not carry semantics that represent applications' needs. Therefore, a layer of indirection that maps the high-level application semantics to low-level addresses has to be introduced to resolve this mismatch.

The IP model also complicates the realization of data-centric security solutions. Today's Internet supports channel-based security, because it fits IP's point-to-point communications. However this class of solution do not secure data itself, therefore data loses protection as soon as it comes out of the channel. In addition, IP addresses are not permanent identifiers that can be used to authenticate remote parties. Therefore a global PKI is needed which certifies the *ownership of DNS names* of individual parties. The PKI is made of a collection of Certificate Authorities (CAs) whose business is selling certificates. This is in sharp contrast to NDN's security model where communicating entities decide the trust relations with each other, instead of through commercial third parties.

The root cause of the above fundamental limitations is that IP-based solutions lack application semantics in the network. Consequently, applications' needs on data security are currently filled by either add-on mechanism for IP, i.e., IPSec, or the layers above, i.e., TLS in combination with CAs. However access to CAs requires stable infrastructure support, which is likely unavailable to vehicular applications, or other types of mobile networking scenarios.

4 EXPLORING A NEW DIRECTION FOR MOBILE NETWORKING

As discussed above, the challenges in vehicular networking call for a data-centric solution where communication is focused on the information desired. In other words, instead of establishing and maintaining connections, vehicles can simply request the desired information as soon as any connectivity becomes available, obtain the desired data through name-based forwarding, and ensure the authenticity of received data via cryptographic verification and reasoning on names.

4.1 Exploring the Data-Centric Solution Space

In our example scenarios, the red vehicle is interested in safety information about a given intersection without needing to know which specific node may have this information. A solution to this problem should address the following issues: (1) how the vehicle can express its data needs, (2) where the network can obtain the desired data, and (3) how the vehicle can verify the authenticity of any received data.

4.1.1 Naming Data. For the red vehicle to obtain the safety information about a specific intersection, it should be able to specify the intersection and the kind of traffic or road information it desires. Therefore, the vehicle's request can include the following parameters:

- *Application Identifier*: This is the desired type of application. For example, this identifier can be *v2safety* for safety applications mentioned in §2.
- *Intersection Identifier*: This unique identifier, determined by geolocations, allows the requester to express the specific intersection that it needs information about. Additionally, it allows forwarders to decide which direction to forward the packet. When finer granularity information beyond the intersection is needed, additional identifiers may be added. For example, a requester may wish to know the traffic situation in a specific lane.

Note that the above is an illustrative example. The corresponding response could also carry information beyond what is requested, to allow the requester to make well-informed decisions. For example, the response may contain the *timestamp* of the information.

Ideally, each vehicle, smartphone, or infrastructure device that receives a request for information should quickly decide whether it can provide the information, and, if not, forward the request further. As such, the information needed for making forwarding decisions must be made visible to the network forwarding process. A remote analogy is that an HTTP URL names an object on the web, and a proxy cache can look at the URL to decide whether it has the data or needs to forward the request. Here we apply the same concept by using a *well-formed name* at the network layer to request desired information. This requires that a vehicle follow well-established naming conventions to construct a request name composed of the intersection identifier and information type to identify and retrieve events at a given intersection.

4.1.2 Stateful Name-Based Forwarding. Depending upon the available connectivity, distance between vehicles, and availability of networking infrastructure (e.g., RSUs), the red car's request may reach a host that can provide the desired data within a single hop. Alternatively, other vehicles and RSUs can re-broadcast the request further in the direction of the intersection. Such decisions can be made by analyzing the *semantical name* in the request, the current GPS position, and map information available to the vehicle.

Furthermore, this safety information can be easily shared with cloud servers to inform commuters in a much broader range. This could be accomplished by having cloud servers periodically request information from vehicles running a driving app, as is already done today. The new "magic" here is seamless information sharing both among vehicles and with the cloud, empowering vehicles with the ability to both request and produce named information, and the ability to forward both requests and replies for other vehicles (Figure 3).

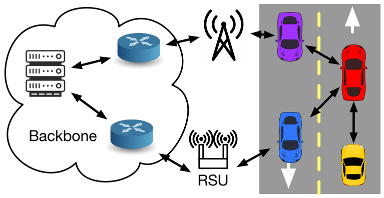


Figure 3: Seamless information sharing among vehicles and with the cloud

By communicating via named information, vehicles and other devices are freed from knowing details about communication interfaces. A request can be received on and the reply (or forwarding of the request) can go out through any interface. If multiple interfaces (e.g., DSRC and Cellular) are available, vehicles can do *stateful forwarding* such that the requests are only forwarded to the more responsive interface. Another advantage of naming desired data using a well-established name structure is that when multiple vehicles request the same information, a forwarder can aggregate them into a single request. When the requested information returns, the broadcast nature of wireless channels, e.g., DSRC, enables all interested parties to obtain a copy. When a request or reply is lost, vehicles still waiting for the information can simply resend the request, with the response coming from some node that has the information, reducing the response time and network traffic.

4.1.3 Ensuring Trustworthy Information. In vehicular networking, one communicates with any nodes it comes across instead of known parties, therefore all received data must be authenticated. This in turn requires producers of data to possess cryptographic certificates, and receivers to be either installed with trust anchor certificates, or be able to fetch them as needed, to verify received data. In addition, when developing solutions for data authenticity and integrity, special care must be taken to protect user privacy. For example, vehicular applications often make use of GPS location information with timestamps, the cryptographic protection of such data must not be associated with information that could trace back to specific drivers/vehicles. Furthermore, one must also keep *usability* in mind when designing vehicular networking with strong security, which implies that the deployed systems must not depend on manual management of cryptographic keys and certificates, that is, they must be automated following the security policies defined by system operators.

In our example scenarios, when a vehicle requests information for a given intersection and receives a notification of a collision generated by an RSU, the requester may verify that the notification is generated by the RSU at the specified intersection with a certificate issued by a trustworthy organization (e.g., the state's Department of Transportation). Such security verification requires pre-installed trust anchor that need out-of-band verification to establish the initial trust, and security policies that are certified by the trust anchor and installed before the system starts.

To sum up our solution space discussion, we have identified three basic needs from the use case: a well defined namespace that one can use to construct requests for desired data, the names can be used directly to bring back the data from anywhere, and the received data carries its own security protection. Although this may sound like a high order, in the next section we explain why we believe this high order is within reach, as a new network architecture, Named Data Networking, can meet exactly these needs.

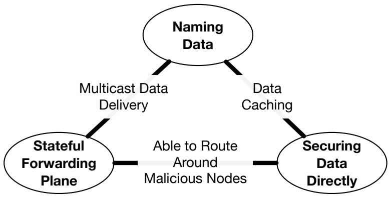
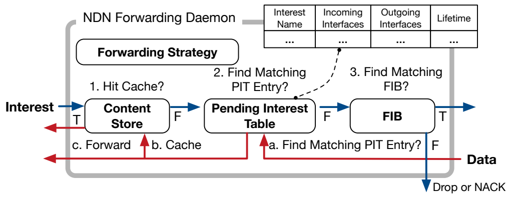


Figure 4: Three pillars of NDN

4.2 Name-based Data Retrieval

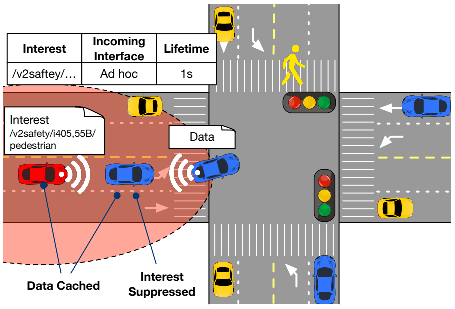
Named Data Networking (NDN) [44] is a proposed new network protocol architecture which has been in development and experimentation since 2010. NDN is built on three simple concepts: *naming data*, *securing data*, and *stateful forwarding plane* (Figure 4). The data names come directly from applications, and NDN uses cryptographic signature to bind the name and its content together. Named, secured data packets are the basic building block in the NDN architecture. Instead of pushing packets to IP destination addresses, NDN lets end applications request desired data by names, and the network brings back named, secured data replies by reversing the path state of the requests. As we show in the rest of this section, different combinations of these three basic components can enable a variety of highly desired functions in vehicular networking.



Interest Name	Incoming Interfaces	Outgoing Interfaces	Lifetime
...	...	...	...

Figure 5: NDN packet forwarding

NDN adopts a name-based data retrieval model: name the desired data and then fetch it using its name. In our example scenarios, data can be named as "`/v2safety/<intersection-id>/<info-type>/<timestamp>`", where the first name component "`v2safety`" is the name of the application and the other name components represent important information that identifies the data, as discussed in §4.1.1. As the requester does not know the exact timestamp of the data, it can send a request with the prefix "`/v2safety/<intersection-id>/<info-type>`" to the network to retrieve any matching data (see Figure 6). In NDN, this request is called an *interest*, and routers then use the interest name, their forwarding table (FIB), and forwarding strategy to forward the interest toward the data producer(s) (see Figure 5). Previously forwarded interests are recorded in a Pending Interest Table (PIT) along with the incoming interface(s) and outgoing interface(s) until the matching data is received, which enables routers to aggregate future interests with the same name and forward data packets back toward the consumer(s). The forwarding state in the PIT also helps routers keep track of the forwarding performance over each outgoing interface, thereby enables the forwarding strategy choosing the best outgoing interface for subsequent interests [42]. If an interest doesn't match any FIB entries, the router can drop the packet, or return the incoming interface with NACK. When the matching *data* is found, it is forwarded toward the consumer on the reverse path of the *interest* and is *cached* on intermediate nodes for future *interests*. A *data* packet matches an *interest* if the *interest* name is a prefix of the data name (they can also match exactly).



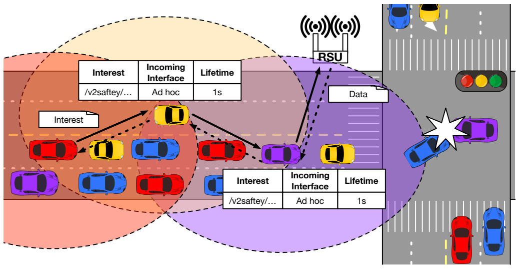
Interest	Incoming Interface	Lifetime
/v2saftey/...	Ad hoc	1s

Figure 6: Interest and data packets in the "Pedestrian in the Intersection" scenario

In the example scenario in Figure 1, the red car broadcasts its *interest* named "`/v2safety/i405,55B/pedestrian`" for any pedestrian information in Intersection 55 (Figure 6). When the blue car closest to the intersection receives the *interest*, it first checks the intersection identifier and information type. Since it has detected a pedestrian at the intersection, it sends back a *data* packet named "`/v2safety/i405,55B/pedestrian/1585086566`" containing the location and other details about the detected pedestrian. This data packet may be received by other vehicles that have expressed *interest* with the same name (e.g., the blue car in front of the red car), and they can use the same data in their decision making. Note that, in order to reduce redundant transmissions, the forwarding process on a vehicle may suppress an outgoing *interest* if the *interest* from the red car carries the same name, but the forwarding process will still maintain state information to match incoming data.

In the example scenario in Figure 2, there is a long line of vehicles due to a collision. Our NDN-based solution can mitigate this problem by having vehicles that are waiting in the line or approaching the line send an *interest* named "`/v2safety/i405,55B/collision`" to check the status of any collisions in the intersection (Figure 7). This *interest* would be forwarded by some of the intermediate vehicles toward the intersection and will eventually reach the RSU at the intersection, which will reply with a *data* packet containing the collision information. The *data* packet will return to the requesting vehicle using the reverse path.

Compared to traditional IP-based approaches, using semantically meaningful names to identify data assists packet forwarding decisions with application contexts, thus avoiding the difficulty of addressing (§3.4) that IP has in mobile networking.



Interest	Incoming Interface	Lifetime
/v2saftey/...	Ad hoc	1s

Interest	Incoming Interface	Lifetime
/v2saftey/...	Ad hoc	1s

Figure 7: Interest and data packets forwarded multiple hops in the "Collision in the Intersection" scenario

4.3 Smart and Robust Forwarding using Names, Forwarding State, and Caching

Semantic data names and stateful forwarding enable NDN to use adaptive forwarding strategies designed for different application scenarios and performance objectives to forward *interests* [42]. As we explain in this section, each vehicle will use a smart forwarding strategy to achieve the performance objectives identified in § 2.

In our example scenarios, the forwarding strategy for the namespace "`/v2safety`" may leverage interest name and geographic information to decide whether to forward the *interest*. For example, as proposed in Navigo [20], the forwarding strategy may use the intersection identifier contained in the *interest* name, the vehicle's current location, and a stored map of the area to determine the vehicle's distance to the target intersection. Then it can set a backoff timer for forwarding the *interest* proportional to the distance (i.e., vehicles with a shorter distance will have a smaller timeout)—whichever vehicle times out first will send the *interest* and the other vehicles will drop their *interests* after hearing that forwarded *interest*. This approach allows vehicles closer to the intersection to time out first and forward the *interest*, which leads to shorter delay and also reduces overall message overhead.

If a vehicle has multiple interfaces, the forwarding strategy can make intelligent decisions about which interface to use for optimal performance. For example, the vehicle can send the same *interest* over both its ad-hoc and cellular interfaces to fetch the desired data – for subsequent requests, it will choose the interface that returns data faster previously. Typically, in our example scenarios, vehicles can obtain desired data faster through their DSRC links. However, if the RSU's DSRC link is having a transient problem, then nearby vehicles' forwarding strategies will switch to using the cellular connectivity to obtain the accident data from the cloud service that collects data from the RSU. This also illustrates that *the NDN-based design can use a single mechanism to retrieve data from both the mobile ad-hoc network and the infrastructure network*. Vehicles can utilize the Pub/Sub API [32] built upon NDN Sync [27] to seamlessly synchronize safety data over multiple interfaces. In contrast, the existing protocol stack on vehicles still lacks multi-interface support. The communication and computation resources on vehicles cannot be fully utilized because of this limitation.

Naming and securing data enable in-network caching that is the key to support robust data sharing under intermittent connectivity. In the "Collision in Intersection" scenario shown in Figure 2, the data from the RSU needs to be forwarded by the purple car and yellow car back to the red car. Suppose the yellow car that previously forwarded the *interest* moves away, then when the purple car sends back the *data*, it will not be further forwarded. The red car will experience a timeout and retransmit its *interest*, which will be forwarded by other vehicles. Since the purple car has the data cached, it will reply the *interest* with matched data in cache, and another possibility is that when the purple car sends back the data (over DSRC broadcast), it will be cached by the downstream blue car as unsolicited data (a caching policy that can be enabled by vehicle owners) so the retransmitted *interest* from the red car will be satisfied by the blue car. In both cases, the number of interest and data packets, as well as the delay in data fetching, is reduced by in-network data caching. In summary, a vehicle can retrieve desired data from any other vehicle that has a copy of the desired data, not just the original producer of the data. As the storage resources on commercial vehicles increase, the cost of caching will become minimal. Essentially, vehicles will become "data mules" that transport data opportunistically, which makes data dissemination robust against connectivity losses.

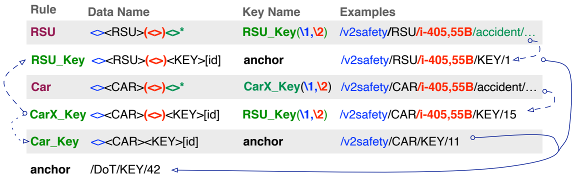
Also, *structured and semantically-meaningful names* facilitates the forwarding. Application requests are directly forwarded toward the data source, without using IP addresses that are difficult to determine on mobile networks. Moreover, data communications in Section 2 can be kept local between senders and receivers, without being sent to a remote rendezvous like clouds.

4.4 Data-Centric Security: Schematized Trust and Automated Key Management

When the requested data can be retrieved from any node (vehicles in our use case), it can be easily forged by an attacker. NDN addresses this problem, by using a key owned by the data producer to generate a *cryptograhic signature* to bind data name and content as part of the data packet [46]. Moreover, the hierarchical data name provide context for deriving trust. Data authenticity can then be verified using the information contained in the data packet, i.e., the data name, content, and signature, as well as a predefined *trust model* that is specific to the application. This data-centric approach to security moves the focus from securing data container/channel/perimeter to *protecting data itself directly*.

The security model, as outlined in §4.1.3, can be captured by a trust schema that matches the names of data produced by RSUs and vehicles with the names of the legitimate keys that sign such data. A simplified version of such a trust schema is shown in Figure 8, which defines several rules to ensure that:

- any data for a specific intersection produced by an RSU must be signed by a key that corresponds to that intersection ("`RSU`"-"`RSU_Key`" relation) identified by the key name;
- an RSU's key for the intersection must be signed by a trusted authority's key – e.g., the Department of Transportation's key ("`RSU_Key`"-"`anchor`");
- any data produced by a vehicle about collisions in an intersection must be signed by a key that matches the intersection ("`Car`"-"`CarX_Key`");
- the vehicle's key for the intersection must be signed (issued) by the RSU at the intersection ("`CarX_Key`"-"`RSU_Key`");
- each car has a key issued by an authority such as the Department of Transportation ("`Car_Key`"-"`anchor`").



Rule	Data Name	Key Name	Examples
RSU	<><RSU>(<>)<>*	RSU_Key(\1,\2)	/v2safety/RSU/i-405,55B/accident/…
RSU_Key	<><RSU>(<>)<KEY>[id]	anchor	/v2safety/RSU/i-405,55B/KEY/1
Car	<><CAR>(<>)<>*	CarX_Key(\1,\2)	/v2safety/CAR/i-405,55B/accident/…
CarX_Key	<><CAR>(<>)<KEY>[id]	RSU_Key(\1,\2)	/v2safety/CAR/i-405,55B/KEY/15
Car_Key	<><CAR><KEY>[id]	anchor	/v2safety/CAR/KEY/11
anchor	/DoT/KEY/42		

Figure 8: Simplified example of a trust schema for Section 2's scenarios

Note that intersection-specific vehicle keys in the figure have two "parents"—RSU and vehicle-specific key—to ensure authenticity and locality of the data. This can be realized when an RSU issues location-specific keys to vehicles. In order to obtain such a key, a vehicle must prove that it has a valid Department of Transportation-issued key. [1]

Based on the above trust model, a *trust schema* containing a set of *trust rules* can be developed to automatically infer correct signing keys for each received data (or key) [43]. Trust rules can be expressed using regular expressions of data names and key names. When a data packet is received, a verification process uses the trust schema to check the following: (1) the key locator field contains a key that is expected by the schema; (2) the key can be retrieved using information contained in the key locator; and (3) the signature matches the data name and content based on the retrieved public key. The verification process repeats these steps for each retrieved key until it reaches the trust anchor whose self-signed public key is pre-configured in the application. If any of these step fails, the data fails verification and is discarded. The required keys can also be generated based on the trust schema. Such schematized trust and automated key management are enabled by structured data names and key names.

To ensure car/driver privacy, safety application can adopt a pseudonym approach similar to Secure Credential Management System (SCMS) [40] (see [12] for NDN-based pseudonym scheme for vehicular networking and in general). In our example scenarios, instead of using a fixed "`CarX_Key`" identity and the corresponding public/private key, cars can obtain a large set of identities (signed by DoT or a dedicated derived authority), which can be used to request intersection-specific keys and secure the published data. NDN makes it easy to use a large number of pseudonym-based keys as it provides built-in support for key distribution. Note that digital signing and encryption are already cheap with current hardware, enforcing verification should not be a problem for vehicular applications.

Unlike IP-based solutions, where deploying data-centric security solutions often require a separate system to manage the mapping between host keys and IP addresses (§3.4), NDN security workflow can be automated via logical reasoning based on the data names, and fetching all necessary keys, certificates, and trust schema in the same way as fetching any named data. NDN addresses security challenges in vehicular networking by utilizing semantically meaningful names of keys and data, which reflect the intrinsic properties in vehicular systems. This represents a fundamentally different approach from blockchain-based security solutions that require external (and potentially expensive) proofs, such as PoW or PoS.

4.5 Same Solution for Diverse Use Cases

The examples we used above focus on intersection safety. There are many other use cases in vehicular networking, such as highway safety and bulk data transfer, which can benefit from the same NDN approach. On a highway, vehicles have to react to problems very quickly due to their high speed. To reduce the potential latency of fetching safety-critical data, each vehicle can persistently keep an *interest* alive. More specifically, whenever the *interest* times out, the vehicle will send another one out so that there is always a pending *interest* in the network for the safety-critical data. In this

[1] We note that certify a producer does not ensure the authenticity of its data content. Cars certified by DoT may still generate fake content. The requirement of an intersection key limits the scope of the content. In the presence of misbehavior, one needs to utilize majority votes to identify true information, and to record all data exchanges to enable later audit to identify misbehavior.

way, safety-critical data will be immediately disseminated to all interested vehicles as soon as it is generated. In addition, popular data, such as traffic congestion data of major roads, fetched by the RSU can be used and authenticated by multiple vehicles.

Beyond the case study (§2) we investigated in vehicular networking, our proposed solution built on NDN also implies how mobile networking can benefit from utilizing semantically meaningful names. This abstraction that unifies the ad-hoc and infrastructure communication with built-in security support is the vision we developed for future mobile computing.

5 DISCUSSIONS AND FUTURE STEPS

In concluding the paper, we would like to first step up a level to examine where we have come from, and then make an informed articulation on the direction we should march toward for the next decade in vehicular networking.

Where we are today. The TCP/IP Internet was developed 40+ years ago for infrastructure based communication. Enabled by computers, packet switching was a revolutionary disruption to circuit-switched telecommunication networks. However, IP's point-to-point communication model, together with naming nodes and pushing packets to destinations, is by and large inherited from telephony. IP is a great design for its time and facilitated explosive advancement in computing technology, which, in turn, extended networking to entirely new territories not envisioned 40 years back - a vast number of inexpensive and capable computing devices all want to communicate with (at least some) other devices, making networking penetrate into every corner that silicon chips have got into: IoT, D2D, M2M, V2V, and many others.

This new landscape has changed the problem of networking to a fundamentally different one from what IP was originally designed to solve. Consequently, new challenges have come along over the years, and network research has branched out to multiple separate divisions. While infrastructure-based networking remains at the core, new branches (e.g., CDN, DTN, MANET, VANET) have been created to address the challenges in specific areas that IP is unable to meet. Sadly, each of these branches explores design options of its own, independently from the others, and similarly to the original IP design, *none* took *security* as an *integral part* in its design.

Why we are here. We believe that this multitude of branching out is due to one root cause: the unfitness of IP's address-based point-to-point delivery model for today's new world. MANET and VANET have no fixed topology or direct end-to-end paths as IP was designed for, and vehicular applications in general care about getting information of road conditions but not which specific device at the location of the interest provides it. The proposed solutions in MANET and VANET areas, by and large, used IP as the starting point and proposed various engineered changes to IP's delivery model. As §3.1 summarized, many also recognized the limitation of IP's delivery model and attempted solutions that depart from the IP model and move towards a data-centric direction. These solutions stagnated at the paper design phase, because they did not recognize that the problems they tried to address come from the architectural incongruity, and it is infeasible to *change* the deployed IP architecture. Consequently, the only *widely deployed* mobility support today is cellular networks that support the last hop mobility, or infrastructure-mode WiFi which disconnects and reconnects a laptop when it moves.

We believe that it is time to recognize the fundamental incongruity between the deployed IP-based solution and the changed problem space, and to understand whether continued engineering patches to the deployed base, including building V2X solutions over TCP/IP model as mentioned in §3.1, can carry the Internet through its next 40 years. Our main contribution in this paper is recognizing that the changed networking landscape requires a change *at the network architecture level.* Bringing discussions to this higher level can serve as the first step toward a future vision for vehicular networking.

Looking forward. This paper promotes a new abstraction for vehicular networking built upon a new network architecture - NDN. In doing so, mobile networking no longer needs special solutions for ad hoc or DTN scenarios, and can unify mobile and infrastructure network designs by communicating semantically named, secured data. The past 10+ years of experimentation with NDN suggests that the *same* NDN network protocol can work effectively in all the network scenarios mentioned above. In particular, NDN's decision of making security an integral part of the design deserves a highlight, as mobile ad hoc networking makes security of ultimate importance.

A frequently raised question is about the feasibility of rolling out NDN, given that the past few decades have witnessed challenges in deploying new technical solutions, such as IP multicast and IPv6. We believe that those deployment challenges are due to the fact that both IP multicast and IPv6 make changes to the existing infrastructure. As a new architecture, NDN will make *no* change to the existing IP infrastructure but simply run on top of it, as well as any other available connectivity technologies to interconnect NDN-capable entities. Furthermore, different from converting functional IPv4 nodes to run IPv6, none of the scenarios described in §2 has available solutions. V2X networking largely represents a green field waiting for solutions to meet the new demands.

As a departing note, we make two points. First, NDN has provided a framework for a new direction of vehicular networking, but that does not mean all problems in going into this new direction have found their final answers. In particular, we note that the namespace design remains as an essential challenge, as, in an NDN network, a name ties to data identification, network forwarding, and security policies[2]. The naming convention of "`/v2safety`" application we showed in Section 4 is only an illustrative example. Although we are convinced that bringing semantic naming into the network layer is the right direction to go, many specifics are yet to be worked out, which is a task that requires the broader community's buy-in and help to move networking toward this exciting new direction. The good news is that a preliminary NDN software infrastructure has been built which includes the forwarding daemon, routing protocols, and security and application libraries, as well as a multi-continental NDN testbed, all of which can be used as a solid starting point to support research endeavors by the community.

ACKNOWLEDGMENT

This work is partially supported by the National Science Foundation under awards CNS-1629769, CNS-1629922 and CNS-1719403.

REFERENCES

[1] 2016. IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services. *IEEE Std 1609.3-2016 (Revision of IEEE Std 1609.3-2010)* (2016), 1–160.

[2] 2019. IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture. *IEEE Std 1609.0-2019 (Revision of IEEE Std 1609.0-2013)* (2019), 1–106.

[3] ISO/TC 204. 2012. Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking. *ISO 21210:2012* (June 2012).

[4] Ikram Ali, Alzubair Hassan, and Fagen Li. 2019. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Vehicular Communications* (2019).

[5] Talar Atechian and Lionel Brunie. 2008. DG-CastoR for query packets dissemination in VANET. In *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*. IEEE, 547–552.

[6] Abdelmalik Bachir and Abderrahim Benslimane. 2003. A multicast protocol in ad hoc networks inter-vehicle geocast. In *The 57th IEEE Semiannual Vehicular Technology Conference, 2003. VTC 2003-Spring.*, Vol. 4. IEEE, 2456–2460.

[7] Ramon Bauza, Javier Gozalvez, and Joaquin Sanchez-Soriano. 2010. Road traffic congestion detection through cooperative vehicle-to-vehicle communications. In *IEEE Local Computer Network Conference*. IEEE, 606–612.

[8] Alina Bejan and Ramon Lawrence. 2002. Peer-to-peer cooperative driving. In *Proceedings of ISCIS*. 259–264.

[9] Bo Xu, A. Ouksel, and O. Wolfson. 2004. Opportunistic resource exchange in inter-vehicle ad-hoc networks. In *IEEE International Conference on Mobile Data Management, 2004. Proceedings. 2004.* 4–12.

[10] Sandra Cespedes, Ning Lu, and Xuemin Shen. 2012. VIP-WAVE: On the feasibility of IP communications in 802.11 p vehicular networks. *IEEE Transactions on Intelligent Transportation Systems* 14, 1 (2012), 82–97.

[11] Yuh-Shyan Chen, Yun-Wei Lin, and Sing-Ling Lee. 2010. A mobicast routing protocol in vehicular ad-hoc networks. *Mobile Networks and Applications* 15, 1 (2010), 20–35.

[12] Muktadir Chowdhury, Ashlesh Gawande, and Lan Wang. 2017. Secure information sharing among autonomous vehicles in NDN. In *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 15–26.

[13] Bruno Defude, Thierry Delot, Sergio Ilarri, Jose-Luis Zechinelli, and Nicolas Cenerario. 2008. Data aggregation in VANETs: the VESPA approach. In *Proceedings of the 5th annual international conference on mobile and ubiquitous systems: computing, networking, and services*. ICST (Institute for Computer Sciences, Social-Informatics and …, 13.

[14] ETSI. 2010. Intelligent Transport Systems (ITS); Security; Security Services and Architecture. *ETSI Technical Specification 102 731* (2010).

[15] TCITS ETSI. 2014. Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols. *ETSI EN* 302 (2014), 636–6.

[16] TCITS ETSI. 2017. Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality. *ETSI EN* 302 (2017), 636–4.

[17] Augustine Ezenwigbo, Vishnu Vardhan Paranthaman, Ramona Trestian, Glenford Mapp, and Fragkiskos Sardis. 2018. Exploring a new transport protocol for vehicular networks. In *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*. IEEE, 287–294.

[18] Samir Goel, Tomasz Imielinski, and Kaan Ozbay. 2004. Ascertaining viability of WiFi based vehicle-to-vehicle network for traffic information dissemination. In *Proceedings. The 7th International IEEE Conference on Intelligent Transportation Systems (IEEE Cat. No. 04TH8749)*. IEEE, 1086–1091.

[19] Fernando Gont, Suresh Krishnan, Dr. Thomas Narten, and Richard P. Draves. 2021. Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6. RFC 8981. https://doi.org/10.17487/RFC8981

[20] Giulio Grassi, Davide Pesavento, Giovanni Pau, Lixia Zhang, and Serge Fdida. 2015. Navigo: Interest forwarding by geolocations in vehicular named data networking. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a.* IEEE, 1–10.

[21] Jinhua Guo, John P Baugh, and Shengquan Wang. 2007. A group signature based secure and privacy-preserving vehicular communication framework. In *2007 Mobile Networking for Vehicular Environments*. IEEE, 103–108.

[22] Harshvardhan P Joshi et al. 2007. Distributed robust geocast: A multicast protocol for inter-vehicle communication. (2007).

[23] John B Kenney. 2011. Dedicated short-range communications (DSRC) standards in the United States. *Proc. IEEE* 99, 7 (2011), 1162–1182.

[24] Maria Kihl, Mihail Sichitiu, Ted Ekeroth, and Michael Rozenberg. 2007. Reliable geographical multicast routing in vehicular ad-hoc networks. In *International Conference on Wired/Wireless Internet Communications*. Springer, 315–325.

[2] Incremental deployment and scalability are often viewed as big challenge too. Due to space limit we will address those issues elsewhere.

[25] Young-Bae Ko and Nitin H Vaidya. 2002. Flooding-based geocasting protocols for mobile ad hoc networks. *Mobile Networks and Applications* 7, 6 (2002), 471–480.

[26] Abderrahmane Lakas and Moumena Shaqfa. 2011. Geocache: sharing and exchanging road traffic information using peer-to-peer vehicular communication. In *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*. IEEE, 1–7.

[27] Tianxiang Li, Wentao Shang, Alex Afanasyev, Lan Wang, and Lixia Zhang. 2018. A brief introduction to ndn dataset synchronization (ndn sync). In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 612–618.

[28] Xingqin Lin, Jeffrey G Andrews, Amitabha Ghosh, and Rapeepat Ratasuk. 2014. An overview of 3GPP device-to-device proximity services. *IEEE Communications Magazine* 52, 4 (2014), 40–48.

[29] Feng Liu and Qi Wang. 2019. IBRS: An Efficient Identity-based Batch Verification Scheme for VANETs Based on Ring Signature. In *2019 IEEE Vehicular Networking Conference (VNC)*. 1–8.

[30] C Maihofer, Christian Cseh, Walter Franz, and Reinhold Eberhardt. 2003. Performance evaluation of stored geocast. In *2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No. 03CH37484)*, Vol. 5. IEEE, 2901–2905.

[31] MN Mariyasagayam, T Osafune, and M Lenardi. 2007. Enhanced multihop vehicular broadcast (MHVB) for active safety applications. In *2007 7th international conference on ITS telecommunications*. IEEE, 1–6.

[32] Philipp Moll, Varun Patil, Lixia Zhang, and Davide Pesavento. [n.d.]. Resilient Brokerless Publish-Subscribe over NDN. In *MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM)*. IEEE, 438–444.

[33] Hamidreza Rahbar, Kshirasagar Naik, and Amiya Nayak. 2010. DTSG: Dynamic time-stable geocast routing in vehicular ad hoc networks. In *2010 The 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*. IEEE, 1–7.

[34] E. Rescorla. 2018. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. RFC Editor.

[35] Masashi Saito, Jun Tsukamoto, Takaaki Umedu, and Teruo Higashino. 2007. Design and evaluation of intervehicle dissemination protocol for propagation of preceding traffic information. *IEEE Transactions on Intelligent Transportation Systems* 8, 3 (2007), 379–390.

[36] Muhammad Sameer Sheikh and Jun Liang. 2019. A Comprehensive Survey on VANET Security Services in Traffic Management System. *Wireless Communications and Mobile Computing* 2019 (2019).

[37] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang. 2010. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems* 21, 9 (2010), 1227–1239.

[38] Yoonyoung Sung and Meejeong Lee. 2012. Light-weight reliable broadcast message delivery for vehicular ad-hoc networks. In *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*. IEEE, 1–6.

[39] Manabu Tsukada, Ines Ben Jemaa, Hamid Menouar, Wenhui Zhang, Maria Goleva, and Thierry Ernst. 2010. Experimental evaluation for IPv6 over VANET geographic routing. In *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*. 736–741.

[40] U.S. Department of Transportation. [n.d.]. Security Credential Management System (SCMS). Online: https://www.its.dot.gov/resources/scms.htm.

[41] Shibin Wang and Nianmin Yao. 2017. LIAP: A local identity-based anonymous message authentication protocol in VANETs. *Computer Communications* 112 (2017), 154–164.

[42] Cheng Yi, Alexander Afanasyev, Lan Wang, Beichuan Zhang, and Lixia Zhang. 2012. Adaptive forwarding in named data networking. *ACM SIGCOMM computer communication review* 42, 3 (2012), 62–67.

[43] Yingdi Yu, Alexander Afanasyev, David Clark, kc claffy, Van Jacobson, and Lixia Zhang. 2015. Schematizing Trust in Named Data Networking. In *Proceedings of the 2nd ACM Conference on Information-Centric Networking* (San Francisco, California, USA) *(ACM-ICN '15)*. Association for Computing Machinery, New York, NY, USA, 177–186. https://doi.org/10.1145/2810156.2810170

[44] Lixia Zhang, Alexander Afanasyev, Jeffrey Burke, Van Jacobson, kc claffy, Patrick Crowley, Christos Papadopoulos, Lan Wang, and Beichuan Zhang. 2014. Named Data Networking. *SIGCOMM Comput. Commun. Rev.* 44, 3 (07 2014), 66–73. https://doi.org/10.1145/2656877.2656887

[45] Lei Zhang, Chuanyan Hu, Qianhong Wu, Josep Domingo-Ferrer, and Bo Qin. 2015. Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response. *IEEE Trans. Comput.* 65, 8 (2015), 2562–2574.

[46] Zhiyi Zhang, Yingdi Yu, Haitao Zhang, Eric Newberry, Spyridon Mastorakis, Yanbiao Li, Alexander Afanasyev, and Lixia Zhang. 2018. An Overview of Security Support in Named Data Networking. *IEEE Communications Magazine* 56, 11 (November 2018), 62–68. https://doi.org/10.1109/MCOM.2018.1701147