Hindawi
Mobile Information Systems
Volume 2018, Article ID 5672154, 11 pages
https://doi.org/10.1155/2018/5672154

Review Article

Security and Privacy Issues in Vehicular Named Data Networks: An Overview

Hakima Khelifi,[1] **Senlin Luo**,[1] **Boubakr Nour**,[2] **and Sayed Chhattan Shah**[3]

[1]*School of Information and Electronics, Beijing Institute of Technology, Beijing, China*
[2]*School of Computer Science, Beijing Institute of Technology, Beijing, China*
[3]*Department of Information Communication Engineering, Hankuk University of Foreign Studies, Seoul, Republic of Korea*

Correspondence should be addressed to Senlin Luo; luosenlin2012@gmail.com

Received 6 July 2018; Accepted 30 August 2018; Published 30 September 2018

Academic Editor: Mohamed Elhoseny

A tremendous amount of content and information are exchanging in a vehicular environment between vehicles, roadside units, and the Internet. This information aims to improve the driving experience and human safety. Due to the VANET's properties and application characteristics, the security becomes an essential aspect and a more challenging task. On the contrary, named data networking has been proposed as a future Internet architecture that may improve the network performance, enhance content access and dissemination, and decrease the communication delay. NDN uses a clean design based on content names and Interest-Data exchange model. In this paper, we focus on the vehicular named data networking environment, targeting the security attacks and privacy issues. We present a state of the art of existing VANET attacks and how NDN can deal with them. We classified these attacks based on the NDN perspective. Furthermore, we define various challenges and issues faced by NDN-based VANET and highlight future research directions that should be addressed by the research community.

1. Introduction

During the past two decades, research academies and industrials focused their attention on vehicular ad hoc networks (VANETs) [1] in order to provide safety and assistance applications, improve the driving experience, and control the road traffic. Towards this goal, several protocols are proposed such as dedicated short-range communication (DSRC), wireless access in vehicular environment (WAVE), and other protocols that run as an overlay on DSRC/WAVE rather than the IP protocol [2]. In a vehicular environment, a huge amount of data are exchanged under different types of communication such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and with pedestrian, satellite, charging stations, and smart grids (V2U). V2I communication can be used in applications that support Internet access, while V2V is mostly used in real applications that need to send emergency and real-time information about an accident or traffic information [3].

However, exchanging information and sharing data in VANET under the use of IP protocol have been a challenging task [4] due to the nature of this network that frequently and quickly changes under the use of poor-quality wireless link which makes VANET more complex in terms of routing, mobility, and security. Also, due to the fact that vehicles may exchange personal and sensitive information, securing the content and communication and preserving user and data privacy are indispensable [5]. VANET communication must ensure different security requirements including privacy, confidentiality, integrity, and nonrepudiation.

Meanwhile, different solutions have been proposed in the literature as future Internet architectures [6]. Information-centric networking (ICN) [7] has been proposed as one of the promising paradigms to replace the current host-centric network. Hereby, many solutions under the name of ICN have been implemented, such as named data networking (NDN) [8]. NDN replaces the IP address with the name of the content and implements a simple content discovery and data delivery mechanism using an Interest-Data exchange model. NDN aims to improve that data dissemination and facilitates content access. Also, it may enhance mobility support and intermittent connectivity

challenge that are difficult to provide through traditional IP networks, by merely re-requesting any unsatisfied request during the mobility and enabling vehicles to retrieve content from the most convenient cache store. Additionally, NDN follows a content-based security concept by protecting the content at the packet level instead of the communication channel level.

Security and privacy are one of the most critical aspects of the whole Internet and not only VANET. Bringing NDN in the vehicular environment has already been introduced in the literature [9]. However, most of the existing works focus on the NDN forwarding plane [10, 11] where the security solutions are rarely elaborated.

1.1. Motivation and Main Contributions. Despite the existing efforts on security, most of them did not consider the nature of VANET communication and attacks in their study [12]; they generally focused on denial of service (DoS) ignoring other attacks. Thus, the main motivation behind this work is to discuss and uncover VANET attacks and security issues from the NDN perspective. Also, as ICN/NDN and VANET merging is still on its first stage and taking a shape, it is quite important to focus on the security and privacy concerns in this phase. It is worth noting that we take VANET as the main network environment, studying its security issues using NDN as a communication model, and not the inverse. To our best knowledge, our work is the first one focusing on VANET security using NDN as a communication plane. Thus, we classify all existing VANET attacks and issues based on the NDN point of view. We overview each one of them and map it to NDN communication. Also, we provide research directions aiming to overcome these attacks and helping the research community to investigate more in this context.

1.2. Organization of the Paper. The rest of the paper is organized as follows: in the following section, we discuss the transaction from current host-centric vehicular networks toward the information-centric paradigm and overview the VANET and NDN architecture, focusing on security issues. Then, in Section 3, we categorize each VANET attack from the NDN perspective and present the existing efforts and summary for each category. Later, we highlight various future research directions in Section 4 and conclude our paper in Section 5.

2. From Host-Centric to Information-Centric Vehicular Networks

ICN is a new communication paradigm that aims to replace the current host-centric model. Shifting from the current IP-based solutions to ICN is not an easy task. Table 1 provides a comparison of host-centric and information-centric paradigms. Regardless of the deployment and transaction methods, mapping ICN communication logic to the existing Internet applications and networks needs more investigation. In this section, we present a quick overview of both VANET and NDN and discuss the mapping between them and the advantages that can be ported by NDN to the vehicular environment. Also, as this work focuses on security, we discuss also some of the security issues related to NDN design.

2.1. Vehicular Ad Hoc Network Overview. Vehicular ad hoc network (VANET) [13] is a part of mobile ad hoc network (MANET) where the node could be a *vehicle* or *roadside unit* (RSU) [14]. Vehicles exchange data with other vehicles (V2V), with RSU (V2I), or with charging stations, personal communication devices, and smart grids (vehicle to uniform) using different VANET applications. Each type of application has its particular features regarding content properties and the way the VANET applications consume it. These characteristics make VANET a challenging environment in terms of security and privacy.

2.1.1. VANET Security and Privacy Problems. As in any communication domain, security requirements in VANET should guarantee authentication, nonrepudiation, integrity, data availability, and confidentiality [15] in order to protect the exchanged messages in the network from modification, deletion, and delay by attackers. The vehicular communication characteristics and application properties have major effects on the security and privacy and make a more challenging environment. The security challenges caused by VANET characteristics are the following:

(1) *Scalability*. VANET is considered as an unbounded network that can be scalable from a small town to a big city until country [16]. It is growing larger and faster with no authority which makes the security enforcement and standardized rules and policies more challenging.

(2) *Mobility*. Due to the high speed of vehicles, the VANET topology can face quick and frequent changes, especially on the highway. Therefore, a very short connection duration and frequently disconnection may occur. Hence, it is very hard to prevent malicious nodes and mitigate attacks in time.

(3) *Time Constraints*. One of the most important of VANET's use cases is safety applications that aim to prevent crashes when an accident happens. These applications require reliable and real-time message delivery. However, due to the possibility of launching denial of service attacks, providing such time constraint services needs more efforts.

(4) *Data Dissemination*. Most of the information and messages in VANET are usually disseminated through vehicles; herein, several applications are vulnerable to attacks to modify, delete, or resend the information at the inappropriate time.

(5) *Privacy*. Preserving data and user privacy is an open issue in the whole Internet including VANET. Vehicles should trust the sender that may have an identity or not, as well as trust the intermediate forwarder vehicles. Thus, trade-off mechanisms are

Table 1: Comparison of host-centric and information-centric models.

Aspect	Host-centric model	Information-centric model
Addressing	(1) Host addresses (2) DNS for host resolution	(1) Content name (2) No DNS required
Routing	(1) Sends packets to the destination address (2) Stateless data plane (3) Point-to-point connectivity (4) Maintains one routing table (5) Routing is based only on the next hop information	(1) Uses Interest packets to fetch the data (2) Stateful data plane (3) Supports multipoint connection (4) Maintains three tables: FIB, PIT, and CS (5) FIB table contains multiple-hop information
Security	(1) Secures the communication channel	(1) Secures the content (content-based security)
Caching	(1) No caching concept	(1) Buffers data packets and reuses them
Mobility	(1) Resends packets to destination addresses	(1) Uses in-network caching and fetches data packets from the most convenient cache point

required between anonymity communication and privacy with the possibility to show real vehicle identity.

2.2. Named Data Networking Overview. Named data networking (NDN) [17] is a promising ICN architecture [18] that follows the content-based paradigm. NDN uses the content name to forward and deliver data between consumers and a producer, with a clean design based on the Interest-Data exchange model. Data packets are sent by a producer/replica node only when receiving an Interest packet triggered by the consumer for the existing content. Both Interest and Data packets contain the same content name.

Every NDN node maintains three data structures: content store (CS), pending interest table (PIT), and forwarding information base (FIB). The CS maintains the locally cached data that can be served for future requests, while the PIT is used to track the received Interest packets, aggregate them, and forward the Data packet downstream. It maintains *content name*, *list of incoming interfaces*, and *nonce* tuple. Similar Interests for the same requests are aggregated within the same PIT entry by pending only the received interface, whereas the FIB table acts as the routing database that contains a list of reachable prefix-names with the outgoing interfaces.

2.2.1. NDN Working Principle. Interest packets are triggered by consumers to discover the content in the network that can be satisfied by either a replica node or the original content producer, where a Data packet is used to deliver the content. Thus, the NDN working principle can be divided into two phases: Interest forwarding and Data forwarding, as illustrated on the right side in Figure 1:

(1) *Interest Forwarding*. When an NDN node receives an Interest packet, it checks its CS whether it already has the requested content. If the content exists on the CS, a Data packet is sent back using the same interface from where the Interest has arrived. Otherwise, PIT exact match is done. When a match is found, it means the same request has already been treated, and the interface name from where the Interest has been received will be appended to the PIT entry; otherwise, a new PIT entry is created for that request by recording the content name and the incoming interface and then performing the FIB longest prefix-name lookup: if a match is found, the Interest will be forwarded to the appropriate interface; otherwise, based on the network policies, the Interest will be either dropped or broadcasted to all interfaces.

(2) *Data Forwarding*. When a Data packet is created by a replica node or the original producer, it carries the same name as in the Interest packet. Hence, the NDN node checks its PIT to verify if the requests have already been treated by him; if a match is found, the Data packet will be sent out to all interfaces listed in the PIT entry (multicast). Otherwise, the packet is considered an unsolicited packet and dropped immediately by the node. During the Data forwarding, the node decides based on its local caching policies, if the content should be cached or not.

It is important to highlight here that all NDN components (CS, PIT, and FIB) are involved in the Interest forwarding phase, while only PIT and CS are used in the Data forwarding.

2.2.2. Security and Privacy in NDN. Preserving data security and preserving user privacy are the most important aspect of any of the today's network architecture and protocol [19]. As the content in NDN is decoupled from its original location, NDN follows a content-based security concept [20] that consists of securing the content among different network elements regardless of the used communication channel:

(1) *Security*. To ensure data authenticity, every Data packet is signed by the original producer using a public key. Thus, any node in the network can verify the data authenticity. Moreover, as Data can be cached in any place in the network, all necessary security-related information is traversed with the Data packets. Furthermore, data confidentiality and access control are supported by content encryption.

(2) *Privacy*. As compared to IP-based networks, any intermediate node can monitor user activities, by knowing who is requesting and what has been requested. However, in NDN, due to the use of

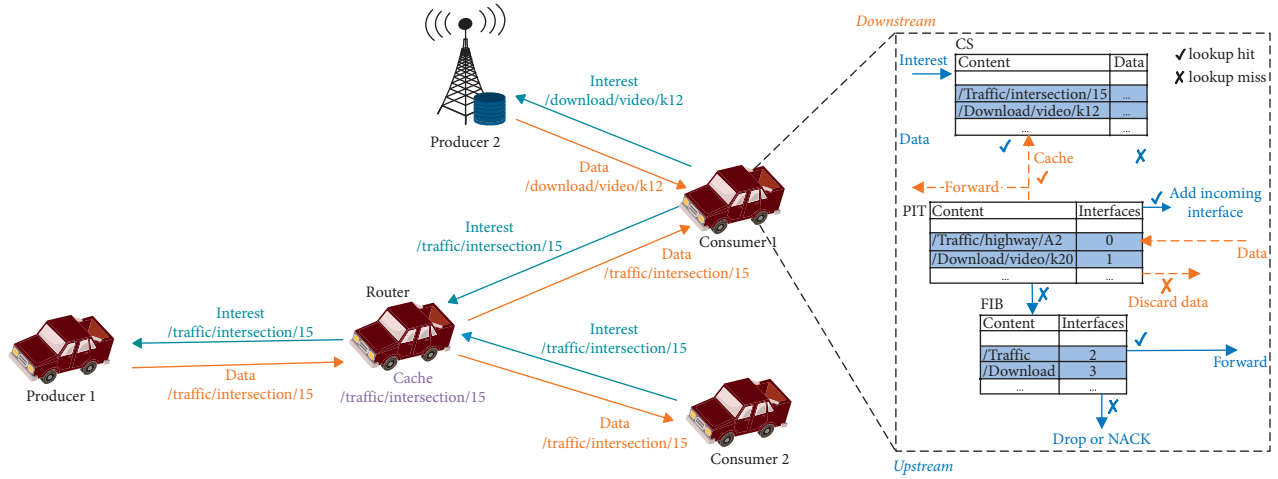

Figure 1: NDN-based VANET.

content names instead of host address, it is not an easy task to know who is requesting, but it is quite easy to know the requested content by monitoring the content names, where various attacks may be launched from different network levels using this vulnerability. Thus, both content and its name should be encrypted to provide high-level privacy.

2.3. NDN Advantages in VANETs. Due to the change of user and application requirements in today's Internet, NDN aims to improve the network scalability and reliability. Towards this, various efforts have been shown tending to bring NDN to vehicular environments [21, 22]. Vehicles in such a merging network can act as data consumers, producers, and intermediates nodes at the same time. Figure 1 shows an example or running NDN architecture on top of the VANET network.

2.3.1. Content Naming. NDN offers a clean, simple, and scale design that can support a large amount of content exchange among vehicles and with infrastructure. Hierarchical NDN names provide a wide addressing range that can be customized by network designers and carry different application semantics [23, 24]. Hence, different application properties can be integrated into the naming scheme to enhance the communication and improve users' needs.

2.3.2. Data Forwarding. The clean content discovery and data delivery mechanisms in NDN make it a suitable solution for VANET [25–27] that can improve the content access among multiple consumers by aggregating the Interests in the first edge node and inherently support multicast communication without the need of extra management protocols. Also, native support of multiple physical interfaces at the same time promotes the necessity of NDN.

2.3.3. In-Network Caching. The time and location decoupling concept in NDN enhances the data availability and improves the overall network performance [28–30]. Data producers are not required to be connected all time to satisfy consumer requests, where the network layer can fulfill different demands especially the hot ones, by retrieving the content from the most closer cache stores.

2.3.4. Data Security. NDN is a session-less architecture, where no session is required to fetch the content from producers or cache store. Also, all security mechanisms are applied to the content itself, by binding the content with its name using the public-private key concept. Hence, securing the communication channel in NDN is not an issue [31].

2.3.5. Mobility Enhancement. By using only the content name to fetch content from the network, NDN aims to enhance node mobility [32]. Mobile nodes are not required to ask for a new address when connecting with the new network. They only need to resend the nonsatisfied Interest by specifying the content name.

3. Security and Privacy Challenges in NDN-Based Vehicular Networks

By moving from a host-centric model to the information-centric concept and using NDN as the primary communication model in VANET, most of the traditional networking aspects will be changed. This also leads to changes in the security and privacy concerns [20]. Also, as ICN/NDN is still taking a shape, more issues will appear when running a large-scale NDN-VANET or fully deployed NDN without overlay protocols. Thus, it is very important to focus on security and privacy in the first design phase. In this section, we first discuss the security and privacy issues in the NDN architecture, and then we classify the existing VANET attacks based on NDN and target only those attacks affecting networking and NDN aspects such as content, routing and forwarding, and caching.

3.1. NDN Security and Privacy Issues. Despite the efforts shown in the NDN project and the research contributions, different security issues still exist in NDN [19]. In the following, we discuss briefly the most critical security issues.

As the network layer takes the responsibilities to satisfy the consumer requests via the ubiquitous in-network caching, different attacks may be launched from different network layers and entities for various goals such as interest flooding attack (due the use of content name), content poisoning attack, and cache poisoning/pollution attack (in-network caching). Hence, the NDN layer should tackle DoS attacks and validate the requested content name.

3.1.1. Content-Name Binding. The content name is the pillar element in ICN/NDN. All network-layer functionalities such as routing, forwarding, mobility, and security are based on the content name. The security of names reflects the network security. In NDN, content and name are bound and validated using the cryptographic function (e.g., public key and signature). Using this secure binding may prove the content ownership. However, in a large-scale network, content may be assigned to different names, which will affect the network scalability especially the routing plane. Thus, a secure control plane to assign names and validate content ownership is required.

3.1.2. Architecture Design. Despite the clean NDN architecture design, some security issues may occur. As NDN communication is based on content name where no host addresses are included, the use of one single interface such as a wireless interface on a vehicle or another device may create a problem of looping in both Interest and Data packets. Even adding a sequence number may solve this problem, however, and according to in-network caching, any node in the network may satisfy the demands. Assuming a malicious node receives all other demands because of the explicit broadcast, it can reply with false content and satisfy these demands, and other nodes in the same rang will receive the Data packets, that by consequence remove the PIT entry where the correct data will be considered unsolicited and dropped by the NDN forwarding plane. In such a scenario, the original requester receives wrong data and will never receive the correct content. Another issue can occur on a node with multiple interfaces: as the Data forwarding plane involves only PIT, a Data packet can be delivered from an interface not indexed in the FIB table but valid on the PIT. Malicious nodes may use this vulnerability to purge all demands on PIT.

3.1.3. Coexistence Issues. NDN can be deployed in three different modes: (a) overlay mode: running NDN on top of the TCP or IP protocol as an overlay layer; (b) coexistence with IP: a node may use the two stacks IP and NDN; and (c) clean-slate mode that consists of running NDN directly. The security of each mode depends on the security of the layer (e.g., IP or TCP). However, to show the real performance of NDN, a clean-slate deployment is required.

In the following sections, we classify VANET attacks into three categories: infrastructure attacks, content protection and access control, and content and user privacy. We overview each attack from both VANET and NDN perspectives and provide a review of existing solutions available.

3.2. Infrastructure Protection. Protecting the infrastructure will by consequence provide high availability and resilience by guaranteeing that only the accurate data are available. Although NDN does not address the hosts directly, securing the infrastructure hosts and endpoints is intuitive, as they are responsible for providing the content. Furthermore, as NDN allows a distributed content caching, this by consequence will increase the content availability and mitigate DoS attacks, which is not always applicable in case of dynamic content that may be generated dynamically only by its original provider.

3.2.1. Denial of Service. Denial of service (DoS) attack [33] is the most famous and dangerous one in the vehicular network, where the attackers send huge requests to the system in order to shut down the network and stop the communication between vehicles and between vehicles and RSUs. The goal of DoS is to stop sending or receiving information to vehicles about the network such as road status.

As NDN deals with content names instead of IP addresses, DoS attacks are based on the use of names [34] and may target consumers, producers, or intermediate nodes. From the NDN point of view, a basic DoS attack can be an *Interest flooding*, where an attacker sends a storm of Interest asking for a different content that may not be available in the cache store.

Figure 2 depicts a simple DoS attack; vehicles, RSUs, and other network infrastructure elements are involved in this scenario. However, due to the *Interest aggregation* feature, intermediate nodes may have more chance to be targeted compared to the content provider, especially when requesting a fake content (i.e., content with a valid name prefix and invalid suffix). The result of that is Interest dropping at the provider level and PIT entries after lifetime expiration at the intermediate nodes level. However, requesting a dynamic content that should be generated by the original content provider upon receiving the Interest (e.g., asking for a fresh patient report) may cause DoS at the provider level due to the fact that dynamic content is not popular and may not be aggregated by intermediate nodes.

A malicious vehicle sends a storm of different Interests asking for different content names, as RSU does not have the content, and it forwards the request and creates a new PIT. Because of the huge number of malicious Interests, the PIT is fitted, where a legitimate vehicle cannot send more requests, and may not benefit of the cache capabilities of the RSU or event forwarding its requests to other nodes. The attack is more severe when it comes to sensitive and urgent communications that may affect people's life.

Various countermeasure solutions have been proposed to overcome and mitigate DoS attacks, by using either rate-limiting mechanisms (e.g., per face or per name-prefix)

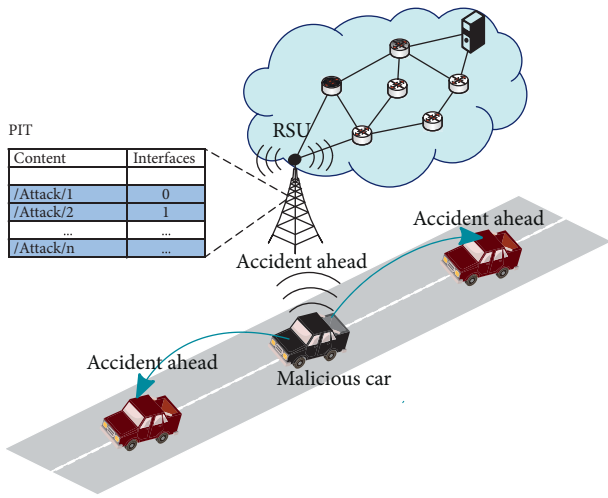

Figure 2: Denial of service attack.

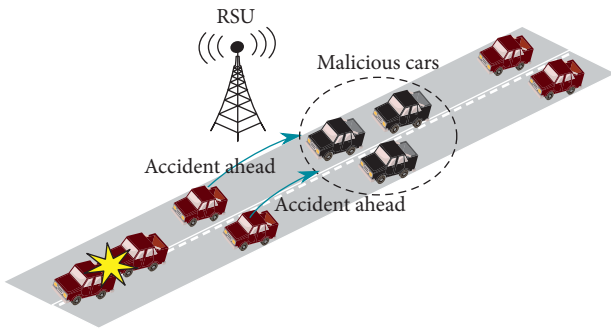

Figure 3: Black-hole attack.

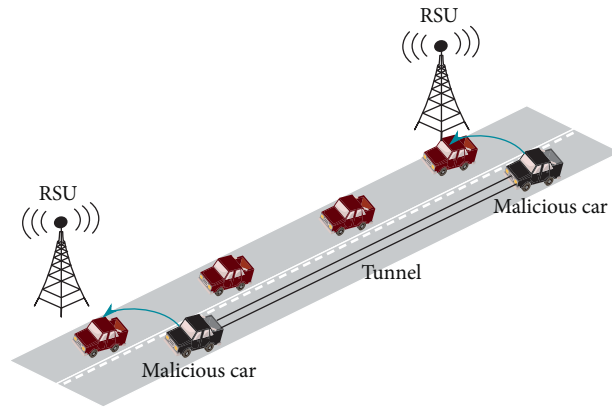

Figure 4: Wormhole attack.

In a nutshell, NDN uses a name-based forwarding scheme to forward the requests and deliver data back to consumers. Solving the black-hole and gray-hole attacks can be achieved either by securing the forwarding plane itself or by using secure namespaces to forward name-prefixes that do not exist in the FIB table. Furthermore, as the NDN forwarding plane forwards Interest/Data packets without knowing who is requesting or who will serve, these attacks may not affect VANET-based NDN even by announcing that they have the best route. However, as NDN uses hierarchical names to identify content and services, a malicious node can easily monitor the forwarding system and filter based on content names that allowed and denied packets, which makes these attacks hard to solve in such cases especially when a group of malicious vehicles launches the attack.

[35, 36] or statistical modeling approaches [37, 38]. The former consists of monitoring the face/name-prefix timeout rates and/or the PIT size, when detecting a DoS attack, and the router limits the interest arrival rate (IAR) on the suspicious face, while the latter relies on statistical information about the PIT and interfaces to identify the abnormal traffic pattern. However, these solutions need to make an extensive modification of the regular PIT structure or excessive storage statistics.

3.2.2. Black-Hole and Gray-Hole Attacks. Another dangerous attack, shown in Figure 3, that especially affects safety applications is the black-hole attack [39], where vehicle attackers engage other vehicles by claiming that they have the best route to the destination or have the best position to forward the packet. After the other vehicles send their packet to attackers, the malicious vehicle discards all packets from the network which caused lose of huge packets including critical information and safety messages. Similarly to the black-hole attack, in gray-hole attack, malicious vehicles act as black nodes and misguiding packets, filtering them according to their benefits. A single malicious node or a set of malicious nodes selects some packets to forward and drops others.

3.2.3. Wormhole Attack. The wormhole attack consists of creating a tunnel between two or more collaborative malicious vehicles, aiming to record and transmit data packets between them. Similarly to the black-hole attack, malicious vehicles engage other neighbor vehicles about the link between them as the best path to fetch the data instead of using the original trust path. After malicious vehicles receive packets from victim vehicles (Figure 4), they encapsulate and tunnel to another malicious vehicle, where the latter opens the encapsulated packets and spreads them in the network. The main objective of this attack is to change the network logical topology and make lose the important information that is sent through the tunnel, as well as creating a private network among the malicious vehicles. In an IP-based network, attackers use their IP addresses to create the tunnel. However, due to the use of names instead of addresses and forwarding packets without the need to know who is requesting and to whom should forward, wormhole attack may not be successfully executed in NDN-based networks.

3.2.4. Man-in-the-Middle Attack (MiMA). In man-in-the-middle attack, a malicious vehicle in the communication path keeps listing to all traversed information and injects

false information between vehicles. This attack, as shown in Figure 5, has serious effects on the safety applications especially if the injected information is about accidents that may cause life-endangering accidents.

Thanks to the content-based security, all information is signed by the original producer during its creation, and any changes in the data payload during the communication will be exposed to changes in the original signatures [40].

3.2.5. Summary and Insight. In this section, we have reviewed the existing VANET attacks that may affect the network infrastructure including DoS, black-hole, worm-hole, gray-hole, and man-in-the-middle attacks. We found that because of using the content name instead of host addresses, many issues can be overcome, especially when binding the content name with the shared information. Also, providing content security at the packet level enhances the communication security.

3.3. Content Protection. As each Data packet is self-signed in NDN, content requesters verify the content signature before consuming the content. Signature verification can also be done by intermediate nodes. However, it will cost more overhead and communication delay. The content signature may ensure *data integrity*, *authentication*, and *correctness*.

3.3.1. Bogus Information. In this type of attack, a malicious vehicle may generate false or wrong information and send it to the network in order to manipulate other vehicles. We find other attacks that can be classified as bogus information attacks, such as the following:

(1) *False Position Information*. Most of the safety applications are based on the particular position, where broadcasting false position information is a hard and critical issue in VANETs. A strong trust and validation model is needed to prevent such false information.

(2) *GPS Spoofing*. A malicious node utilizes the GPS satellite simulator to produce signals which are stronger than the actual satellite signals, tending to deceive vehicles to accept the false position information. This attack is related to physical devices. However, NDN should deal with trust in such data propagation, where collaborative vehicles may detect this information and stop it.

(3) *Illusion Attack*. Attackers disseminate wrong messages to create an illusion to vehicles by exploiting the current road conditions, like a group of cars moves slowly in order to deceive drivers to believe in this wrong information. This attack is hard to detect as the physical vehicle's sensors are used to create and spread the wrong traffic information.

Bogus information attack is usually associated with authentication security conditions, which is an easy task to deal with NDN, as the content is protected and authenticated at the packet level with a secure content-name binding

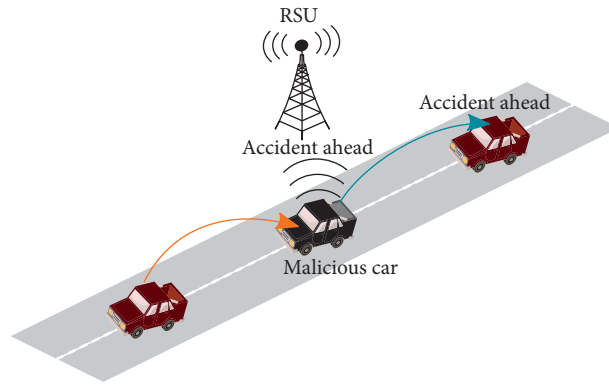

Figure 5: Man-in-the-middle attack.

of mechanisms based on hashing techniques and public-private keys.

3.3.2. Replay Attack. In the replay attack, a malicious vehicle saves a copy of the message and resends it later in the network in order to deceive other vehicles, making unnecessary stopping. As NDN is a cache-based network, this attack can be overcome by using the content name and checking the lifetime value in Data packets to know the data freshness, compared with the requested content.

3.3.3. Summary and Insight. Most of the existing NDN attacks related to content in VANETs can be solved by following the content-based security concept. Indeed, securing the content after its creation helps the content security life cycle. Also, when securing the content, access control rules and policies can be used to enforce who can access the content. Moreover, a robust trust model with the validation system is required in NDN to enforce content security and mitigate false content created by malicious nodes.

3.4. Content and User Privacy. Regardless of the content protection level, the user and content privacy still can be compromised in NDN, especially by using plain-text names. Any malicious node may receive the traversing requests and data back. By monitoring the content names, attackers can create a fake content and cache it in any near cache store, that by consequence will be served for future requests.

3.4.1. Sybil and Masquerade Attacks. Sybil attack is considered as one of the most dangerous attacks in VANETs, where the malicious vehicle acts that it is more than a hundred vehicles by creating chaos and a large number of pseudonymous as shown in Figure 6. The goal of this behavior is to deceive other vehicles that there is congestion and force them to change their routes. On the contrary, as the name indicates, in a masquerade attack, a malicious vehicle changes its identity [41] to be another vehicle, trying to produce different messages, alter, and replay with information to deceive other vehicles. For example,

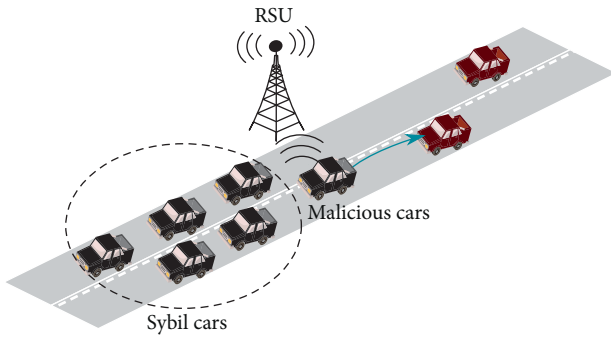

Figure 6: Sybil attack.

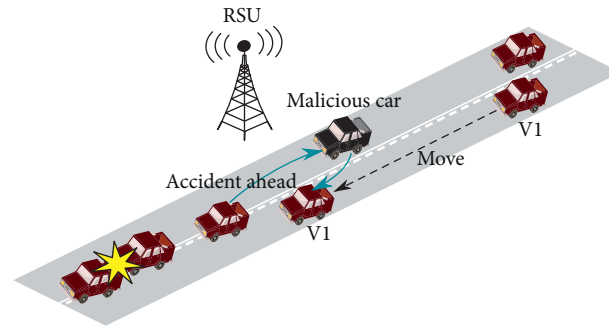

Figure 7: Timing attack.

a malicious vehicle can change its identity to be an ambulance and force other vehicles to slow down or change their routes. Works in [42, 43] propose a trust model based on NDN for autonomous vehicular applications in order to prevent bugs information and vehicle tracking. The authors designed a hierarchical naming scheme that composed of four levels: *autonomous vehicle*, *manufacturers*, *vehicles*, and *data*. Furthermore, they used a pseudonym and proxy-based scheme in order to make it difficult for attackers to track vehicles.

NDN binds content names using cryptography algorithms such as public-private keys that may secure the binding and outdo these issues. Furthermore, distributed solutions such as blockchain can be applied to enforce the content-name binding and preserve content and user privacy.

3.4.2. Timing Attack. In timing attacks, the malicious vehicles do not forward the emergency messages and information at the right time (Figure 7) they received it, by creating an explicit communication delay and adding time slots to the received messages. Their neighbor's vehicles receive these messages too late after the time they need it. The timing attack is a critical issue, especially when dealing with time-constraint applications.

3.4.3. Snooping Attack. Snooping is a passive attack, where the malicious vehicle accesses the content and information that traverse it, in order to use it for its benefits without modification. However, as the content is secure and signed, using cryptographic hashing techniques, when it has been created, only legitimate users can access it. Hence, snooping attack may not have an effect on VANET-based NDN.

3.4.4. Summary and Insight. Content and user privacy issues are presented in this part. Content privacy can be preserved using the content-name-binding mechanisms, and more investigation is required in such a context. Also, due to the illumination of host addresses, monitoring attacks can be decreased. The only issue that can occur because of NDN names is the caching-related attacks. Finally, serious solutions and secure forwarding schemes are required to overcome the timing attacks.

4. Future Research Directions

Based on the presented security attacks and issues and their relation with NDN, in the following section, we identify several NDN research directions that may enhance and improve the security of the NDN architecture. Table 2 summarizes this discussion.

4.1. Denial of Service. Solutions based on limiting Interest rate on the malicious interfaces or based on name-prefixes may end by punishing legitimate consumers and authorized requests. Hence, using the software-defined networking (SDN) approach [44] may detect DoS attack in the early stages using the global view of controllers and a per flow rate limiting that may yield highest fairness compared to interface/name-prefix-based solutions. Also, the core routers can collaborate to identify and filter the malicious name-prefixes and malicious traffic pattern using AI-based algorithms.

4.2. Content Poisoning. The purpose of this attacker is to fill the node's cache stores with fake contents. All the existing solutions require performing a data packet signature verification at the intermediate nodes level, that affects the content retrieval delay; comparing content hash with the hash taken from the corresponding Interest may reduce the network scalability, or ranking the content using consumers' feedback, where attackers also have the chance to send malicious feedbacks.

4.3. Naming and Content-Name Binding. Providing a secure naming scheme is still an open research challenge for ICN and NDN. A secure naming scheme should ensure an efficient and scalable binding between the name and the content that may avoid various types of attacks. All the existing binding schemes require signature verification for each and every data packet. This process is costly in terms of resources, as well as affects the data retrieval delay, where an intermediate node cannot perform it at the line speed rate.

4.4. Caching Pollution. The main objective of the caching pollution attack is to diminish the operation of in-network caching and augment content retrieval latency. The existing

Table 2: Summary of issues and research directions.

Category	Attacks	Compromised services	Target NDN aspects	Possible directions
Infrastructure protection	DOS	(1) Authentication (2) Availability	(1) Routing and forwarding plane	(1) Interface-based rate limit (2) Name-based rate limit (3) Statistical rate limit
	Black-hole and gray-hole	(1) Availability	(1) Routing and forwarding plane	(1) Securing the forwarding plane (2) Use of secure namespace
	Wormhole	(1) Confidentiality	(1) Data packets	(1) Use of content names instead of device identifications (2) Performing name-based forwarding
	Man-in-the-middle	(1) Authentication (2) Confidentiality (3) Integrity (4) Nonrepudiation	(1) Data packets (2) Forwarding plane	(1) Content-based security mechanism (2) Securing the content during the creation (3) Attaching access control policies with content
Content protection	Bogus information	(1) Authentication (2) Integrity	(1) Data plane	(1) Securing the content using cryptographic hashing techniques and public-private keys
	Replay	(1) Authentication (2) Integrity	(1) Data packet (2) Cache store	(1) Fetching content from the cache store based lifetime (2) Requesting only the fresh content
Content and user privacy	Sybil	(1) Authentication (2) Availability	(1) Routing and forwarding plane	(1) Securing content-name binding (2) Preserving blockchain-based identity
	Masquerade	(1) Authentication (2) Nonrepudiation (3) Integrity	(1) Routing and forwarding plane	(1) Preserving blockchain-based identity
	Timing attack	(1) Availability	(1) Data packets (2) Caching store	(1) Securing the forwarding plane (2) Trust-based forwarding scheme (3) Reputation-based caching and forwarding
	Snooping attack	(1) Authentication	(1) Data packets	(1) Applying content-based security mechanisms (2) Adding access rules within Data packets

solutions have a high computation overhead at intermediate nodes. We consider a collaborative caching scheme a suitable solution to help the core network to mitigate this attack by exchanging feedback between cache stores, keep only the popular content, and reduce the nonpopular ones.

4.5. Secrecy of Correspondence. Preserving the SoC and content copyrights is one of the most critical privacy topics in the whole networking domain and not only ICN [31]. From SoC perspectives, the content owner should state all privacy and content-use policies in the Data packet or in the content itself. We believe that the blockchain-like structure combined with the smart contract can be one of the promising solutions. The content owner specifies different smart contracts depending on the policies such as caching, providing, and consuming the content, that may be executed automatically when the action is triggered, to enforce SoC and content copyright.

4.6. Application Design Patterns. Several application-level security mechanisms have been proposed in ICN such as the following: (i) request filtering that intends to identify and remove the unwanted or forged content from untrusted providers, by using provider's information (e.g., public keys and name-prefix) and consumers' votes for content ranking. (ii) Anomaly detection aims to detect unwanted activities or network misbehavior, using statistical data analyses, fuzzy detection algorithms, and traffic clustering. However, there is no all-in-one scheme that deals with the existing application-level threats or discusses the design patterns for a secure application in ICN, which is a strong future research topic.

5. Conclusion

NDN architecture is a suitable candidate for the future Internet, including vehicular communication. Deploying NDN on top of VANET is still in the early phase. Security and privacy issues have a strong impact on the success of such merging. This article addresses the major networking security and privacy issues in VANET from the perspective of the NDN communication model. The nature of VANET communication and applications changes the way of seeing security; also, adding the NDN model on VANET makes the task more challenging. We categorized VANET security

challenges and discussed them from the NDN perspective. Also, we highlighted different NDN research directions and guidelines.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Hankuk University of Foreign Studies Research Fund of 2018 and National Research Foundation of Korea (2017R1C1B5017629).

References

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, 2014.

[2] F. Cunha, L. Villas, A. Boukerche et al., "Data communication in VANETs: protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90–103, 2016.

[3] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: challenges, architectures, and future directions," *Vehicular Communications*, vol. 9, pp. 268–280, 2017.

[4] T. Mekki, I. Jabri, A. Rachedi, and M. B. Jemaa, "Proactive and hybrid wireless network access strategy for Vehicle Cloud networks: an evolutionary game approach," in *Proceedings of 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1108–1113, IEEE, Valencia, Spain, June 2017.

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: a survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[6] J. Pan, S. Paul, and R. Jain, "A survey of the research on future internet architectures," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 26–36, 2011.

[7] A. V. Vasilakos, Z. Li, G. Simon, and W. You, "Information centric network: research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 52, pp. 1–10, 2015.

[8] L. Zhang, A. Afanasyev, J. Burke et al., "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[9] Z. Su, Y. Hui, and Q. Yang, "The next generation vehicular networks: a content-centric framework," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 60–66, 2017.

[10] M. A. Yaqub, S. H. Ahmed, S. H. Bouk, and D. Kim, "Interest forwarding in vehicular information centric networks: a survey," in *Proceedings of 31st Annual ACM Symposium on Applied Computing-SAC'16*, pp. 724–729, ACM, Pisa, Italy, April 2016.

[11] S. H. Bouk, S. H. Ahmed, D. Kim, K.-J. Park, Y. Eun, and J. Lloret, "LAPEL: hop limit based adaptive PIT entry lifetime for vehicular named data networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5546–5557, 2018.

[12] S. Signorello, M. R. Palattella, and L. A. Grieco, "Security challenges in future NDN-enabled VANETs," in *Proceedings of 2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 1771–1775, IEEE, Tianjin, China, August 2016.

[13] S. Boussoufa-Lahlah, F. Semchedine, and L. Bouallouche-Medjkoune, "Geographic routing protocols for Vehicular Ad hoc NETworks (VANETs): a survey," *Vehicular Communications*, vol. 11, pp. 20–31, 2018.

[14] D. Kim, Y. Velasco, W. Wang, R. Uma, R. Hussain, and S. Lee, "A new comprehensive RSU installation strategy for cost-efficient VANET deployment," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4200–4211, 2017.

[15] H. Sedjelmaci and S. M. Senouci, "Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution," *Journal of Supercomputing*, pp. 1–17, 2018.

[16] M. Laroui, A. Sellami, B. Nour, H. Moungla, H. Afifi, and S. Boukli-Hacéne, "Driving path stability in VANETs," in *IEEE Global Communications Conference*, Abu Dhabi, UAE, December 2018.

[17] L. Zhang, D. Estrin, J. Burke et al., *Named Data Networking (NDN) Project*, Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC, Palo Alto, CA, USA, 2010.

[18] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, 2012.

[19] T. Chatterjee, S. Ruj, and S. D. Bit, "Security issues in named data networks," *Computer*, vol. 51, no. 1, pp. 66–75, 2018.

[20] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: a survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 566–600, 2018.

[21] M. Amadeo, C. Campolo, and A. Molinaro, "Content-centric networking: is that a solution for upcoming vehicular networks?," in *Proceedings of Ninth ACM international Workshop on Vehicular inter-networking, systems, and applications*, pp. 99–102, ACM, New York, NY, USA, November 2012.

[22] S. H. Bouk, S. H. Ahmed, D. Kim, and H. Song, "Named-data-networking-based ITS for smart cities," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 105–111, 2017.

[23] S. H. Bouk, S. H. Ahmed, and D. Kim, "Hierarchical and hash based naming with compact trie name management scheme for vehicular content centric networks," *Computer Communications*, vol. 71, pp. 73–83, 2015.

[24] B. Nour, K. Sharif, F. Li, H. Moungla, and Y. Liu, "M2HAV: a standardized ICN naming scheme for wireless devices in internet of things," in *Proceedings of International Conference on Wireless Algorithms, Systems, and Applications*, pp. 289–301, Springer, Guilin, China, June 2017.

[25] X. Liu, Z. Li, P. Yang, and Y. Dong, "Information-centric mobile ad hoc networks and content routing: a survey," *Ad Hoc Networks*, vol. 58, pp. 255–268, 2017.

[26] M. F. Majeed, S. H. Ahmed, and M. N. Dailey, "Enabling push-based critical data forwarding in vehicular named data networks," *IEEE Communications Letters*, vol. 21, no. 4, pp. 873–876, 2017.

[27] S. H. Ahmed, S. H. Bouk, M. A. Yaqub, D. Kim, and H. Song, "DIFS: distributed interest forwarder selection in vehicular named data networks," *IEEE Transactions on Intelligent Transportation Systems*, 2017.

[28] M. A. Yaqub, S. H. Ahmed, and D. Kim, "Asking neighbors a favor: cooperative video retrieval using cellular networks in VANETs," *Vehicular Communications*, vol. 12, pp. 39–49, 2018.

[29] H. Khelifi, S. Luo, B. Nour, A. Sellami, H. Moungla, and F. Naït-Abdesselam, "An optimized proactive caching scheme based on mobility prediction for vehicular networks," in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Abu Dhabi, UAE, December 2018.

[30] B. Nour, K. Sharif, F. Li, H. Moungla, A. E. Kamal, and H. Afifi, "NCP: a near ICN cache placement scheme for IoT-based traffic class," in *Proceedings of IEEE Global*

Communications Conference (GLOBECOM), pp. 1–6, Abu Dhabi, UAE, December 2018.

[31] C. Ghali, G. Tsudik, and C. A. Wood, "When encryption is not enough: privacy attacks in content-centric networking," in *Proceedings of 4th ACM Conference on Information-Centric Networking*, pp. 1–10, ACM, Berlin, Germany, January 2017.

[32] J. M. Duarte, T. Braun, and L. A. Villas, "Source Mobility in Vehicular Named-Data Networking: An Overview," in *Proceedings of 9th EAI International Conference on Ad Hoc Networks*, pp. 83–93, Springer, Niagara Falls, ON, USA, March 2018.

[33] S. M. Specht and R. B. Lee, "Distributed denial of service: taxonomies of attacks, tools, and countermeasures," in *Proceedings of 17th International Conference on Parallel and Distributed Computing Systems*, pp. 543–550, San Francisco, CA, USA, September2004.

[34] M. Aamir and S. M. A. Zaidi, "Denial-of-service in content centric (named data) networking: a tutorial and state-of-the-art survey," *Security and Communication Networks*, vol. 8, no. 11, pp. 2037–2059, 2015.

[35] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *Proceedings of 2013 IFIP Networking Conference*, pp. 1–9, IEEE, Brooklyn, NY, USA, May 2013.

[36] H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate ddos attacks in NDN by interest traceback," in *Proceedings of 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 381–386, April 2013.

[37] K. Wang, J. Chen, H. Zhou, and Y. Qin, "Content-centric networking: effect of content caching on mitigating dos attack," *International Journal of Computer Science Issues*, vol. 9, no. 6, pp. 43–52, 2012.

[38] T. Nguyen, R. Cogranne, and G. Doyen, "An optimal statistical test for robust detection against interest flooding attacks in ccn," in *Proceedings of 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 252–260, IEEE, Ottawa, Canada, May 2015.

[39] F.-H. Tseng, H.-P. Chiang, and H.-C. Chao, "Black hole along with other attacks in MANETs: a survey," *Journal of Information Processing Systems*, vol. 14, no. 1, 2018.

[40] C. Ghali, A. Narayanan, D. Oran, G. Tsudik, and C. A. Wood, "Secure fragmentation for content-centric networks," in *Proceedings of IEEE 14th International Symposium on Network Computing and Applications (NCA)*, pp. 47–56, IEEE, Cambridge, MA, USA, 2015.

[41] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[42] M. Chowdhury, A. Gawande, and L. Wang, "Anonymous authentication and pseudonym-renewal for VANET in NDN," in *Proceedings of 4th ACM Conference on Information-Centric Networking*, pp. 222-223, ACM, Berlin, Germany, January 2017.

[43] M. Chowdhury, A. Gawande, and L. Wang, "Secure information sharing among autonomous vehicles in NDN," in *Proceedings of Second International Conference on Internet-of-Things Design and Implementation*, pp. 15–25, ACM, Pittsburgh, PA, USA, April 2017.

[44] A. Alioua, S.-M. Senouci, S. Moussaoui, H. Sedjelmaci, and A. Boualouache, "Software-defined heterogeneous vehicular networks: taxonomy and architecture," in *Proceedings of Global Information Infrastructure and Networking Symposium (GIIS)*, pp. 50–55, IEEE, Saint Pierre, Reunion Island, France, October 2017.