Breaking Geographic Routing Among Connected Vehicles

Zizheng Liu
Department of Computer Science
Purdue University
West Lafayette, IN, USA
lzz@purdue.edu

Shaan Shekhar
Department of Computer Science
Purdue University
West Lafayette, IN, USA
shekhar5@purdue.edu

Chunyi Peng
Department of Computer Science
Purdue University
West Lafayette, IN, USA
chunyi@purdue.edu

***Abstract*—Geographic routing for connected vehicles enables vehicles and roadside infrastructure to exchange information about traffic conditions and road hazards based on their geographic positions. Its security is thus critical to traffic efficiency and road safety. In this paper, we conduct a security analysis of one standardized geographic routing protocol – `GeoNetworking`– and unfortunately find that its packet forwarding algorithms are vulnerable to two simple attacks. The first *inter-area interception attack* disturbs the victim vehicle's routing decision making and intercepts packets transmitted from one area to another. The second *intra-area blockage attack* intervenes packet forwarding within an area by impersonating a packet forwarder in a contention based flooding process; The attacker injects fake packets to its nearby peers and prevents vehicles within an area from receiving the broadcast packets. We use an open-source simulator to evaluate the effectiveness of proof-of-concept attacks and assess their attack damages under the settings released in public field tests. The first attack achieves an inter-area interception rate up to 99.9% (>35% in all test cases); The second attack reaches an intra-area packet blockage rate between 35% and 39%, which implies that about one-third vehicles within an area fail to receive broadcast packets. These attacks cause unnecessary traffic jams and collisions which could be avoided if `GeoNetworking` is properly secured. We further propose standard-compatible solutions to mitigating both attacks and conduct a preliminary evaluation to validate their effectiveness.**

***Keywords*—Geographic Routing; Connected Vehicles; GeoNetworking; Interception Attacks**

I. Introduction

Geographic routing is an essential technique for a vehicle to exchange information with other vehicles and roadside infrastructure based on their geographic positions [1]–[3]. As illustrated in Figure 1, a source vehicle (marked in blue) wants to disseminate a packet to its nearby nodes; The vehicle specifies its destination area (say, within a range radius r) and then floods the packet to its direct neighbors which further forward the packet hop by hop until it exceeds the specified destination area. As a result, vehicles get connected over geographic routing, which plays a vital role in enhancing traffic efficiency and road safety. For example, a vehicle broadcasts a warning about its emergent braking to its surrounding vehicles to avoid collisions; Or roadside infrastructure forwards traffic jam information to vehicles approaching the jam to stop them from entering the blocked road.

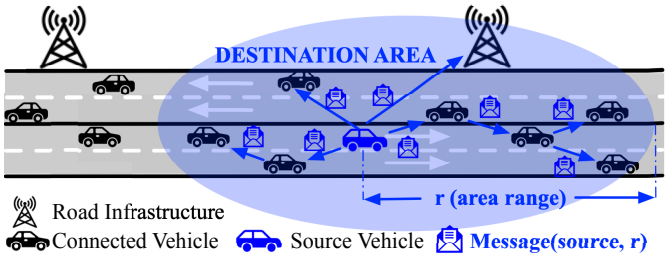


Fig. 1: Illustration of geographic routing via `GeoNetworking`.

In recent years, geographic routing has been actively studied, particularly with a steady step toward standard making and commercialization. In January 2020, European Telecommunications Standards Institute (ETSI) released the latest geographic routing standard for Intelligent Transport Systems, which is referred to as the **`GeoNetworking`** protocol [3]. `GeoNetworking` is also adopted in the US; A network layer standard for connected vehicle communication in the US (called IEEE WSMP) uses `GeoNetworking` features to support geographic routing [4]. Its security mechanism is regulated by another ETSI technical specification (say, TS 102.731 [5]), which supports confidentiality, integrity, authorization, and authentication to secure message exchanges. IEEE (more precisely, IEEE 1609.2 [6]) defines secure message formats and mechanisms (say, certificate management) to protect message exchanges between connected vehicles. A vehicle must acquire a certificate from a certification authority (CA) to communicate with other vehicles or roadside infrastructure.

Despite these security mechanisms, our security analysis shows that `GeoNetworking` is still vulnerable to packet interception attacks. The attacker does not need any certificate from the CA or break the security mechanisms in place. More threateningly, they are outsider attacks with no need of turning participating vehicles into malicious nodes; Instead, the attacks can be launched by a nearby node (say, at the roadside) which can sniff and intercept packets from legitimate vehicles. Different from the known attacks (e.g., blackhole/grayhole attacks [7]) that require the attackers to forge `beacons` to advertise fake positions closer to the destination area, the attacks in this work just need to selectively capture and relay `beacons` or packets from legitimate vehicles. This makes the attacks more

stealthy, bypassing the existing security mechanisms.

The vulnerabilities are rooted in two routing algorithms used by GeoNetworking to forward packets across geographic areas (inter-area) or within a geographic area (intra-area). Specifically, GeoNetworking uses two algorithms: Greedy Forwarding (GF) and Contention-Based Forwarding (CBF) (background detailed in §II). GF is used to explicitly select the next hop vehicle to forward packets from one area to another when the source vehicle is outside the destination area; CBF is used to determine how a vehicle inside the destination area broadcasts packets to its neighbors. We conduct a security check on both algorithms regulated in the standard specification [3] and find that they are vulnerable to packet interception. In particular, we devise two proof-of-concept attacks: *inter-area interception attack* and *intra-area blockage attack*.

In the first *inter-area interception attack*, the attacker intercepts packets forwarded from one area to another. GF asks vehicles to broadcast beacons to advertise their positions to support GeoNetworking features. Because the beacons are never encrypted, the attacker can eavesdrop on the beacons to get the positions of the vehicles within its radio coverage. Afterward, the attacker can capture a beacon from a vehicle and replay it to another vehicle (here, the victim) out of the advertising vehicle's coverage. The victim vehicle that receives the beacon uses the position information in the beacon for packet forwarding, without checking the source of the beacon. As a consequence, the vehicle makes a wrong routing decision and forwards the packet to out-of-coverage vehicles. We notice that authentication is enforced on beacon transmission and reception, which is effective to protect vehicles from blackhole/grayhole attacks [7]. However, authentication cannot prevent the *inter-area interception attack* as the used beacon is valid but abused to cheat the wrong recipients.

In the second *intra-area blockage attack*, the attacker blocks vehicles from receiving packets broadcast within a confined area. It seems hard because the number of vehicles receiving the broadcast packet grows exponentially with the hop number. Specifically, the vehicles within the destination area run CBF to broadcast packets: The first hop vehicle broadcasts the packet to its neighbors; The next hop vehicles do not re-broadcast the packet if they hear back from one of their peers who have already re-broadcast the packet. By exploiting this loophole, the attacker can impersonate a packet forwarder and replay modified packets. The attacker captures the packet from the previous hop and broadcasts it to the current-hop vehicles, thus stopping them from re-broadcasting the packet.

We use an open-source simulator to evaluate the effectiveness of the attacks and assess their damages to road safety and traffic efficiency. To evaluate the attack effectiveness, we simulate both attacks with a variety of active traffic on a 4 km road segment. The traffic and simulation settings are based on public datasets [8], [9]. We test with two common vehicle communication technologies (DSRC [10] and C-V2X [11]). Our evaluation results show that the *inter-area interception attack* intercepts almost all packets with a success rate of 99.9% – 100%; The *intra-area blockage attack* reduces the number of vehicles that receive the broadcast packet by 35.3% – 38.1%. The attacks result in traffic jams and collisions which do not exist in attack-free scenarios.

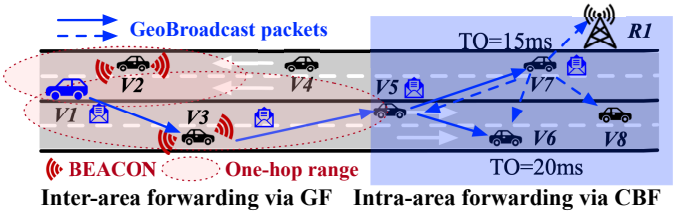


Fig. 2: Illustration of two forwarding algorithms: GF for inter-area forwarding and CBF for intra-area forwarding.

Finally, we propose standard-compatible solutions to mitigate both attacks. We implement our mitigation solutions in the simulator and conduct preliminary evaluations. The results show that they are effective in increasing packet reception rates by at least 53% and 16% under inter-area and intra-area interception attacks, respectively.

II. Background on GeoNetworking

GeoNetworking forwards data packets based on geographic positions (more precisely, destination areas), using a technique called GeoBroadcast [12]. As illustrated in Figure 2, it uses two algorithms – Greedy Forwarding (GF) and Contention-Based Forwarding (CBF) – to handle inter-area and intra-area packet transmission. Vehicles and roadside infrastructure within a destination area (marked in a blue rectangular, here, V5– V8, R1) use CBF to broadcast packets to their neighbors. The nodes outside the destination area (here, V1– V4) do not flood the packet; Instead, they use the GF algorithm to choose its next-hop recipient which further forwards the packet toward the destination area.

Greedy Forwarding (GF) Algorithm. The GF algorithm is used by a forwarder outside the destination area to explicitly select its next-hop recipient. In GeoNetworking, vehicles periodically advertise their positions via beacons. As a result, a vehicle knows the positions of its neighboring vehicles within its one-hop communication range. The GF algorithm chooses the neighbor closest to the destination area based on position information advertised in the beacons from its neighbors.

Figure 2 gives an illustrative example where a vehicle (here, V1) wants to forward the packet using the GF algorithm. V1 receives beacons broadcast from its neighbors (here, V2 and V3) and knows their positions. When V1 needs to forward a packet toward the destination area, it picks V3 as the next hop because V3 is closer to the destination. V1 forwards the packet to V3 which repeats the same process until the packet enters the destination area (here, V3 forwards the packet to V5).

Contention-Based Forwarding (CBF) Algorithm. The CBF algorithm is used for intra-area forwarding which floods the packet to all nodes within the destination area. It runs as follows. The source node broadcasts the packet to its neighbors, which become candidate forwarders upon receiving the packet. A candidate forwarder places the packet into its buffer and starts a timer. The timeout (TO) value is inversely proportional

to its distance from the previous sender. If timeout, the packet is re-broadcast to its neighbors. Evidently, the node closer to the previous sender will re-broadcast the packet later. If a candidate forwarder receives the packet for a second time before its timer expires (within a time $<$ TO), it learns that there exists another forwarder which has already re-broadcast the packet. It thus discards the packet and stops the timer to avoid unnecessary repeated transmissions.

In the example shown in Figure 2, V5 broadcasts the packet within the destination area. Both V6 and V7 are within its communication range and receive the broadcast packet. V6 is closer to V5 and thus sets a larger TO value (here, 20 ms). As a result, V7, with a smaller TO value (here, 15 ms), re-broadcasts the packet which is received by V5, V6, V8 and R1. V6 receives the duplicate packet from V7 and discards the packet in its buffer. V8 and R1 repeat the process to disseminate the packet.

GeoNetworking Security. ETSI specifies common security mechanisms of authorization, authentication, integrity, privacy and confidentiality to protect GeoNetworking [5]. Each vehicle has to activate a long-term or one-off security association (SA) to exchange private messages. This SA enforces all the above security mechanisms. Public messages such as beacons and GeoBroadcast packets, are protected by most security mechanisms of authorization, authentication, and integrity protection (except that confidentiality is not required). A personal vehicle is allowed to use a pseudonym to hide its true identity and protect its privacy.

ETSI and IEEE both advocate certificate management for connected vehicles [5], [6]. Specifically, each vehicle first acquires a certificate with an enrollment request to a CA (e.g., the U.S. Department of Transportation). The certificate is later used to authenticate outgoing and incoming messages. If the authentication fails, the message will not be accepted.

III. Attacks Against GeoNetworking

This section starts with our threat model. We then present two interception attacks, which exploit vulnerabilities identified in both GF and CBF algorithms.

A. Threat Model

Adversaries are organizations or people who attempt to monitor and attack connected vehicles running GeoNetworking through contactless radio channels. There are two attack capabilities and restrictions.

• **Outsider attacker.** No legitimate nodes (connected vehicles or roadside infrastructure) are malicious or compromised. They are protected by standard security mechanisms (say, authorization, authentication, integrity and confidentiality as described in §II). An attacker can deploy its own equipment (say, a radio sniffer over public vehicular communication channels) near the victims to eavesdrop and capture packets within its communication range. The attacker cannot break security measures in place; Namely, the attacker cannot acquire/forge a valid certificate to sign outgoing messages or decrypt encrypted messages without knowing the decryption keys.

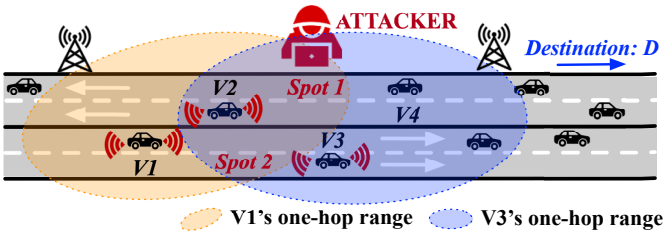


Fig. 3: An illustrative scenario for both attacks. The attacker is deployed in the overlapping coverage areas of V1 and V3 (here, *Spot 1* or *Spot 2*).

• **Active attacker.** The attacker can replay or modify the captured packets without breaking enforced security measures. Specifically, the attacker can extract information from unencrypted messages (e.g., node positions from beacons) and use a pseudonym (allowed for privacy protection) to conceal its identity while sending the same or modified packet.

In this work, we consider *stationary* attackers which deploy their radio sniffers on the roadside. Conceptually, the attacks are applicable to moving attackers (legitimate or illegitimate vehicles) but handling mobility and attack responsiveness is required. The attackers can use publicly available information (e.g., traffic maps [8], [13]) to choose attack locations where victim vehicles are more vulnerable to interception attacks. We consider both line-of-sight (LoS) and non-line-of-sight (NLoS) communications as vehicle communication might be blocked by surrounding vehicles. The attackers can intentionally place their sniffers at higher open spaces on the roadside (e.g., at street light poles) in order to make LoS communication with more on-road vehicles.

B. Attack #1: Inter-area Interception Attack

The first attack exploits vulnerabilities in the GF algorithm to intercept inter-area packet transmission. We describe how this attack works using an illustrative scenario, where a few vehicles, say, V1– V4 and others, on a road segment (Figure 3). The source vehicle (here, V1) is outside the destination area and wants to forward a packet to a destination area (marked as D, not included in Figure 3). V1's one-hop coverage is marked by an orange ellipse, where V2 is within its communication range but V3 and V4 are not.

The attacker is deployed in the overlapped coverage areas of V1 and V3 (here, *Spot 1* or *Spot 2*). It can communicate directly with V1 and V3, as well as V2. It aims to intercept the packet from V1 to D over multiple hops.

GF and its vulnerabilities. As introduced in §II, each vehicle periodically broadcasts beacons to advertise its position information to its direct neighbors. Each beacon contains a position vector (PV) including the vehicle's geographical location, movement speed and heading. According to the ETSI standard [3], a beacon is periodically broadcast every 3 seconds with a random jitter within 0.75 seconds. It uses one-hop broadcast. Every vehicle uses a location table (LocT) to store the PVs of its neighbors, each of which takes one

table entry with three tuples, LocTE (addr, PV, TTL)[1]. Upon receiving a beacon, the vehicle extracts the PV and the source vehicle's access layer address (addr). The addr acts as an ID. If addr is already in LocT, the corresponding LocTE is updated with the new PV. Otherwise, a new LocTE is created. By default, TTL (time-to-live) is set to 20 seconds.

To forward a packet using the GF algorithm, the forwarder (here, V1) calculates the distance from the destination to its neighbors. If the shortest distance is smaller than the distance from itself to the destination, the GF algorithm picks the corresponding neighbor as the next hop. Otherwise, the forwarder either rechecks its LocT later or broadcasts the packet without specifying the next hop.

The above process seems secure with GeoNetworking security mechanisms. For example, in a false position advertisement attack [14], an attacker may claim to be closer to the destination via fake beacons to attract the forwarder to send the packet to it. Such forged beacons will not be accepted in GeoNetworking because the authentication fails. It is not feasible for the attacker to alter PV in a beacon sent by a legitimate vehicle since its integrity is protected.

However, we find the following three GF vulnerabilities which can be exploited to intercept inter-area packet forwarding despite the security mechanisms in place.

- **Beacons are not encrypted.** As broadcast messages, beacons are sent without encryption. As a result, the attacker sniffing the vehicular communication channel knows the positions of the vehicles within its attack range. Moreover, such positions are refreshed approximately every 3 seconds (the broadcast period of beacons). By this means, the attacker can estimate the coverage of these vehicles and further infer whether two vehicles are out of each other's coverage.
- **No plausibility check is performed upon the received beacons and PVs.** The GF algorithm does not require a vehicle to check whether the received beacon is from another vehicle in a plausible distance. The vehicle does check the timestamp to ensure its freshness but never checks the PV contained in the beacon. It simply accepts the beacon although it is replayed by an attacker and originally from an out-of-coverage vehicle (here, V3). Consequently, it likely picks a vehicle outside its communication range as its next-hop forwarder. In this example, V3 is highly likely chosen as the winner given its authentic PV. It is indeed closer to the destination area but just unreachable by V1.
- **No acknowledgment is required for inter-area packet transmission.** It is not without rationale because not using ACK can reduce signaling overhead. However, once a vehicle forwards the packet to another vehicle out of its communication range, it fails to know that the target vehicle does not receive the packet; The packet is lost without being detected.

[1]More tuples are defined in [3] but not used in this work.

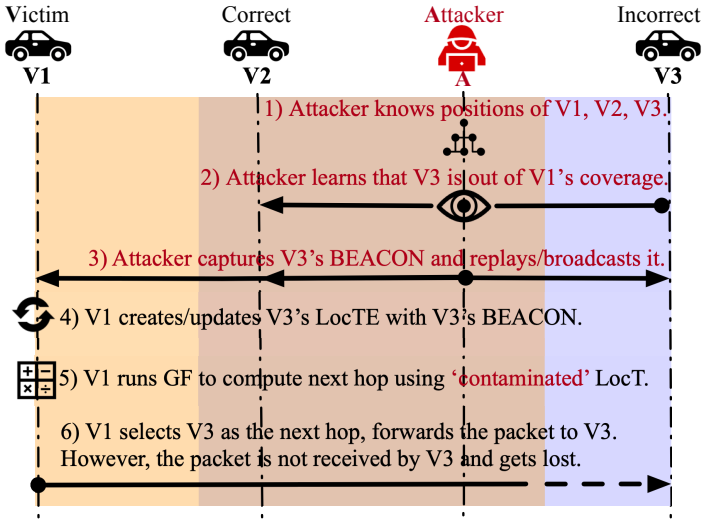


Fig. 4: *Inter-area interception attack*: the attacker replays V3's beacon to cheat V1 to select V3 as the next hop although it is out of V1's coverage. The forwarded packet is intercepted.

Attack procedure. Exploiting the above vulnerabilities, the *inter-area interception attack* is launched with the following steps depicted in Figure 4. Without loss of generality, V1, V2 and V3 in this illustrative example represent the *victim*, *a correct next-hop choice* and *an incorrect next-hop choice*, respectively. That is, V2 is the one closest to the destination area D among all V1's real neighbors. V3 is even closer but is out of V1's communication range. The attacker A is deployed at a location which can reach both V1 and V3.

1) By eavesdropping on unencrypted beacons, the attacker A knows the positions of vehicles V1-V3.
2) A further infers that V1 and V3 are outside each other's coverage when continuously receiving beacons every 3s.
3) A captures the latest beacon from V3 and immediately relays the captured beacon so that V1 receives the packet regardless of that V3 is out of V1's coverage.
4) Upon receiving V3's beacon maliciously broadcast by A, without a distance plausibility check, V1 stores the PV in the LocTE for V3 and labels V3 as a neighbor.
5) When V1 forwards a packet toward D, it runs the GF algorithm to decide the next hop using the PVs stored in the LocT (here, V2 and V3's PVs). As a result, V3 is returned as the winner (a wrong one).
6) V1 forwards the packet to V3. Since V3 is outside V1's coverage and no acknowledgment is required, the packet is intercepted without being detected.

Discussion. We notice that forwarding a packet to an out-of-coverage vehicle happens even in attacker-free scenarios. For example, due to high dynamics of fast-moving vehicles, it is possible that the forwarder fails to reach the next hop although its beacon is heard. Or, the next-hop vehicle selected by GF drives away from the current forwarder's coverage due to its PV stored in the LocT is stale. Nevertheless, we show that their impacts are negligible in presence of the attack in §IV.

In practice, the attacker does not know which vehicle will be

a packet forwarder in advance. Consequently, the attack cannot be launched against a specific vehicle. Instead, the attack is launched as long as two or more vehicles out of each other's coverage are detected from their unencrypted beacons. Such condition is not hard to meet in reality because the attack range can be intentionally enlarged. The attacker can talk to more vehicles as the attacker-to-vehicle communication range can be easily larger than (say, hundreds of meters more than) the vehicle-to-vehicle one.

C. Attack #2: Intra-area Blockage Attack

The second attack exploits vulnerabilities in the CBF algorithm to intervene intra-area packet flooding. We still use the example scenario in Figure 3 to illustrate how the attack works. Different from §III-B, V1 wants to forward the packet to all nodes within the destination area which covers the entire road segment. All vehicles on the road are destination nodes.

The attacker is still located in the overlapped coverage areas of V1 and V3. It can be placed at *Spot 1* or *Spot 2*, as shown in Figure 3. It aims to block the dissemination of the packet before it is received by all vehicles on the road.

CBF and its vulnerabilities. In CBF, a vehicle buffers the received packet and sets a TO value. The TO value is inversely proportional to the distance from the vehicle to the previous sender. Specifically, it is computed as

$$TO = \begin{cases} TO\_MIN, & \text{for DIST > DIST\_MAX} \\ TO\_MAX + \frac{TO\_MIN - TO\_MAX}{DIST\_MAX} \times DIST, & \text{for DIST} \leq \text{DIST\_MAX} \end{cases}$$

where TO_MIN and TO_MAX are the pre-configured minimum and maximum durations the packet shall be buffered; DIST is the distance between the node's and the previous sender's positions, and DIST_MAX is the theoretical maximum communication range of the wireless access technology used (i.e., DSRC or C-V2X). The default values of TO_MIN and TO_MAX are 1 ms and 100 ms, respectively.

If a vehicle with the packet buffered receives a duplicate packet before the timer expires, it stops the timer and discards the buffered packet. A duplicate packet is detected based on the packet's sequence number. If no duplicate packets are received upon a timeout, the vehicle re-broadcasts the packet. The hop limit of the packet is set by a field called Remaining hop limit (RHL) in the packet header; It decreases by one per hop.

Blocking the CBF packet flooding is challenging. Once the source node broadcasts the packet, all vehicles that receive the packet are candidate forwarders. The packet is blocked if *all* candidate forwarders do not re-broadcast the packet. However, we find the following vulnerabilities of the CBF algorithm that the attacker can leverage to block the packet distribution *at least* along one direction of the road segment:

- **Vehicles do not distinguish between hop numbers.** When the n+1th hop vehicles buffering the packet receives a duplicated packet, it cannot distinguish whether the second packet is sent by one of its n+1th hop peers or is sent by the nth hop for a second time. Thus, the attacker can capture and replay the packet from the nth hop to impersonate a n+1th hop forwarder.
- **Vehicles do not verify the source of duplicate packet.** Since the vehicle does not verify the distance between the peer from which it receives the duplicate packet and the previous hop, it blindly believes that the attacker is a forwarder with a smaller TO. Consequently, it discards the locally buffered packet.

Leveraging the above vulnerabilities, an attacker can first capture the packet from the nth hop and immediately broadcast the packet to all nodes in its coverage to impersonate a forwarder with the smallest TO. Upon receiving the duplicate packet, n+1th hop candidate forwarders discard the locally buffered packet.

However, the attacker has to set its communication range large enough to ensure all the n+1th hop forwarders receive the packet. Otherwise, even one missed candidate forwarder will keep forwarding the packet, invalidating the effectiveness of the attack. But if the communication range is set too large, the packet broadcast by the attacker will also be received by vehicles that have yet to receive it. These vehicles, namely, the n+2th hop candidate forwarders, will process the packet as a new packet and keep forwarding it using CBF. Due to the highly dynamic topology of connected vehicle networks, precisely determining the packet receivers by tuning the communication range is impossible.

We further uncover the third vulnerability which makes the attack possible:

- **RHL is not integrity protected.** The RHL field indicating the remaining hop limit of the packet is not integrity protected. Thus, the attacker can change the value of RHL to 1 before broadcasting it without being detected by the receivers. In this way, the attacker only needs to ensure that all n+1th hop vehicles receive the packet without worrying about n+2th hop vehicles because n+2th hop vehicles will decrease RHL to 0 and discard the packet instead of buffering it.

Attack procedure. Combining the above vulnerabilities, we devise a proof-of-concept *intra-area blockage attack* as illustrated in Figure 5. Since V1 cannot reach V3 while V2 can reach both V1 and V3, we use V1, V2 and V3 in the example to represent the nth hop, n+1th hop and n+2th hop, respectively.

1) Attacker A knows the positions of nodes V1-V3 by eavesdropping on their unencrypted beacons. A also infers the communication ranges of V1-V3.
2) V1 (nth hop) broadcasts the packet p to its neighbors, p is received by V2 (n+1th hop) and also captured by A.
3) Upon receiving p, V2 buffers the packet and sets TO_p inversely proportional to its distances to V1.
4) If A is at *Spot 1*, A cannot make the replayed packet, p_A, received by all n+1th hop forwarders without making it received by V3 (n+2th hop), A decreases the RHL of the packet to 1 and broadcasts it as p_A.
5) V2 receives p_A, stops TO_p and discards p from its buffer. The new receiver V3 decreases the RHL by 1 (RHL reaches

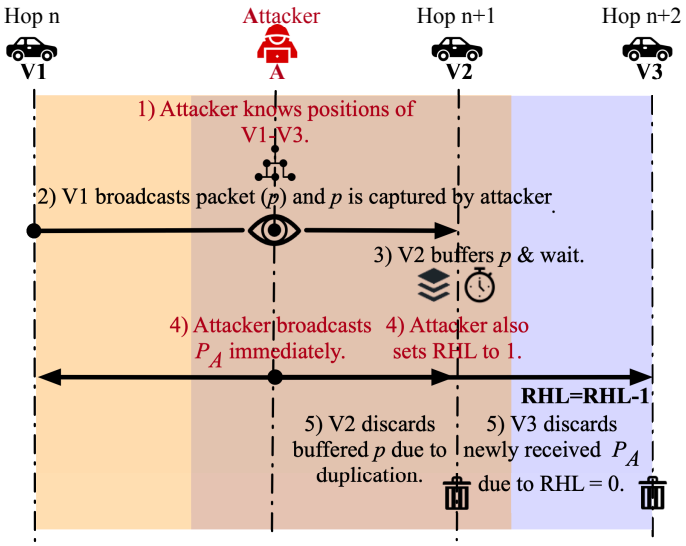


Fig. 5: Intra-area blockage attack: The attacker impersonates a forwarder with smallest TO. It decreases the RHL in the captured packet to 1 and broadcasts it without buffering. Candidate forwards discard the buffered packets due to duplication. New receivers discard the received packet since the RHL reaches 0.

0) and discards p_A.

If A is at *Spot 2*, an *intra-area blockage attack* variant is launched as follows:

1-3) The first three steps remain the same.

4) Becase A is at *Spot 2*, it knows that the packet will be forwarded eastbound *only* through V2; It thus broadcasts the captured packet p_A without modification and makes it received only by V2 by controlling its transmission power.

5) V2 receives the maliciously replayed packet p_A, stops TO_p and discards p from its buffer.

Discussion. The attacker can choose to launch the original attack or its variant, depending on the topology of vehicles in its coverage. A conservative approach is to decrease RHL to 1 and broadcast p_A with its highest transmission power. Although this approach results in more first-time receivers, it reduces the likelihood of missing a candidate forwarder.

The attack time window ranges from 1 ms (TO_MIN) to 100 ms (TO_MAX). Assuming the attacker is able to process packets no slower than legitimate vehicles, we argue that a time window of 1 ms is enough to modify and replay packets in the *intra-area blockage attack*. This matches with previous studies [15], [16].

IV. Evaluation

In this section, we first evaluate the effectiveness of both attacks under different communication and traffic settings. We then run a showcase study to demonstrate negative impacts of the attacks on traffic efficiency and road safety. Both the effectiveness evaluation and impact study are done by simulation. We implement GF and CBF algorithms in an open-source simulator [17]. We implement the attack codes in the simulator to launch the attacks against inter-area and intra-area

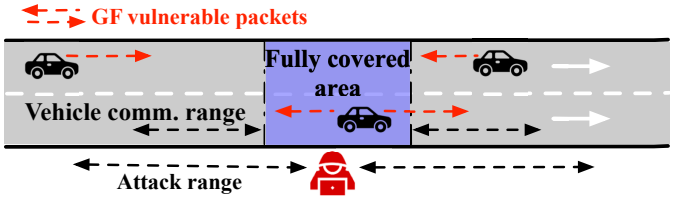


Fig. 6: The attacker is located in the middle of a 4,000-meter road segment. The *fully covered area* is marked in blue.

forwarding. We quantitatively assess the attack damages with regards to various parameters including the communication range of attackers, TTLs of location table entries, and traffic settings. All the parameters are configured based on traces collected in real-world experiments.

A. Attack Effectiveness

Traffic settings and attacker positions. We use a public traffic dataset from Maryland Department of Transportation [8]. The attacks are launched against vehicles in active traffic on a 4,000-meter road segment. We consider both one-way and two-way roads. Each direction has two lanes, and each lane is 5 meters wide. Each vehicle enters the road at a speed of 30 m/s when the vehicle ahead is more than 30 meters away from the road entrance. The road segment length and traffic density are similar to a 3,800-meter road segment of the Baltimore-Washington Parkway as reported in [8]. In [8], there are 94,951 annual average daily traffic (≈1.1 vehicles/second). Each vehicle is 4.5 meters long and uses an intelligent driver model (IDM) [9] for car following. Table I lists the used IDM parameters; Figure 6 shows a one-way scenario (the two-way one skipped due to space limit) where the attacker is located at the center of the road segment.

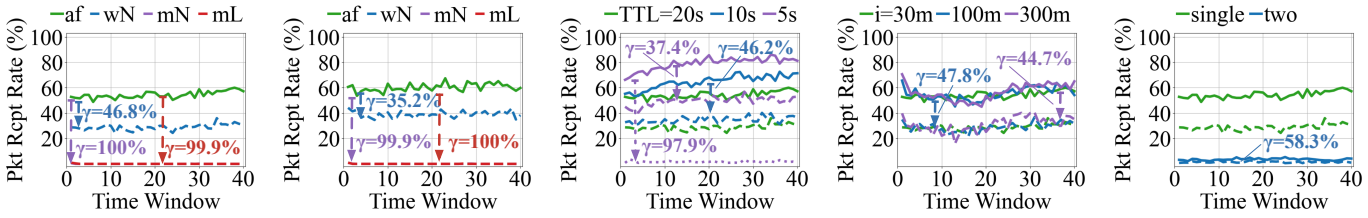
TABLE I: Parameters used for IDM.

Parameter	Value
Desired velocity	30 m/s
Safe time headway	1.5 s
Maximum acceleration	1.0 m/s^2
Comfortable deceleration	3.0 m/s^2
Acceleration exponent	4
Minimum distance	2 m

TABLE II: Communication ranges used for DSRC and C-V2X.

Comm. range	DSRC	C-V2X
LoS (median)	1,283 m	1,703 m
NLoS (median)	486 m	593 m
NLoS (worst)	327 m	359 m

Communication settings. We test with two common vehicle communication technologies: DSRC [10] and C-V2X [11]. We set their communication ranges using another field test by the Utah Department of Transportation [18]. Table II lists their LoS and NLoS ranges. The NLoS range is much shorter (DSRC: 486 m, C-V2X: 593 m). In this work, we consider



(a) Attack range (DSRC) (b) Attack range (C-V2X) (c) LocTE TTL value (DSRC) (d) Inter-vehicle space (DSRC) (e) Number of directions (DSRC)

Fig. 7: The effectiveness of *inter-area interception attack* with different attack ranges (a & b), LocTE TTL values (c), inter-vehicle spaces (d) and the number of directions (e). Solid lines denote the attacker-free scenarios, dashed and dotted lines denote the attacked scenarios. γ indicates the packet interception rates.

NLoS for vehicle-to-vehicle communication because trucks often block the LoS communication between sedans on the highway [19]. In the following evaluation, the attacker changes its transmission power to control its communication range up to the median LoS range.

Simulation settings. In the default simulation settings, we consider vehicles driving in a single-direction, two-lane, 4000-meter road segment; Vehicles are 30 meters apart and TTL is set as 20 seconds for each LocTE. We evaluate the attack effectiveness with various parameters of the attack range, TTL, inter-vehicle space and the number of road directions (single/two). All vehicles and the attacker use the same access layer technology (either DSRC or C-V2X) in each simulation run. Simulations are done with A/B testing whereas A refers to attacker-free scenarios and B refers to the attacked ones. Each setting is tested with 100 runs. Each run lasts for 200 seconds.

Effectiveness of *inter-area interception attack*. We evaluate the attack effectiveness on a road segment, where on-road vehicles transmit packets toward two ends of the road (Figure 6). We set up two static destinations 20 meters beyond each end of this road segment. A packet is treated as a *vulnerable* one if the coverage of at least one forwarder is surpassed by the attacker toward the packet's forwarded direction. Thus, any packet generated from the *fully covered area* (denoted by the blue shade) targeting either destination is a *vulnerable packet*. Besides, eastbound (or westbound) packets generated from vehicles in the area to the west (or the east) of the *fully covered area* are also *vulnerable packets*. Figure 6 shows several *vulnerable packets* (in red dashed lines). Notably, a *vulnerable packet* does NOT need to be generated from a vehicle inside the attack range; A packet is vulnerable to an *inter-area interception attack* as long as any hop between the source and the destination is located inside the attack range.

In each simulation run, a vehicle is randomly selected every second to generate a *vulnerable packet*. The attacker re-broadcasts all beacons that it hears to the vehicles within its communication coverage (i.e., attack range). In each run, we calculate the packet reception rate as the number of *vulnerable packets* received at two destinations divided by the number of *vulnerable packets* transmitted; We show the packet reception rates of attack-free scenarios in solid lines and the packet reception rates of attacked scenarios in dashed or dotted lines in Figure 7. Besides, we also compute the packet interception rate γ as the average drop rate of packet reception rates from attacker-free to attacked scenarios over forty 5 s time bins. We denote γ of each simulation setting in Figure 7.

We first evaluate the attack effectiveness with various attack ranges. Figure 7a and Figure 7b show the packet reception rates and γ under default simulation settings of DSRC and C-V2X communication, respectively. The results of different attack ranges are differentiated by line color. We first set the attack range to the median LoS range (mL) and show results as red dashed lines. Compared with the green solid lines (attacker-free, af), almost all *vulnerable packets* are intercepted regardless of communication technology used (γ=**99.9%** with DSRC, γ=**100%** with C-V2X). We get similar results after shortening the attack range to the median NLoS range (mN) as shown by the purple lines. We then further reduce the attack range to the worst NLoS range (wN). The attack still shows non-negligible effects as shown by the blue line. Specifically, the interception rate γ is **46.8%** using DSRC and **35.2%** using C-V2X, which indicates that DSRC with a shorter communication range is more vulnerable to the *inter-area interception attack*.

Without losing generality, we use DSRC as the communication technology in the following simulation runs. Also to avoid the impact of other parameters being dominated by the large attack range, we set up a worst NLoS range attacker by default in the following simulation runs. A/B test results of different simulation settings are differentiated by line color in the figures of the following runs (Figure 7c-Figure 7e).

Figure 7c shows the attack effectiveness with different LocTE TTL values. Comparing the solid lines (attacker-free tests) and the dashed lines (attacked tests), the results show that the *inter-area interception attack* is effective as the TTL value increases from 5s to 20s. The interception rates are **46.8%**, **46.2%** and **37.4%** when TTL values are 20s, 10s, and 5s, respectively. This indicates that the attack effectiveness decreases as LocTE TTL becomes shorter. This is because the effects of error beacons will be cleared sooner with a shorter

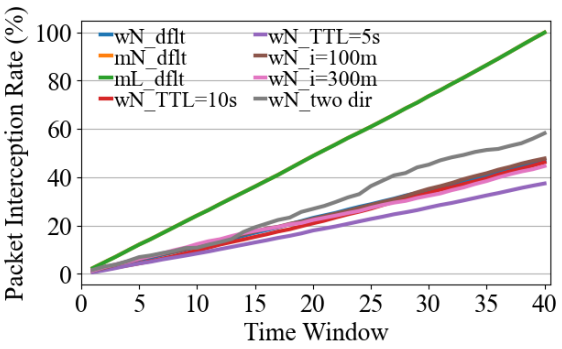


Fig. 8: The overall effectiveness of the *inter-area interception attack* in different scenarios using DSRC.

LocTE expiration time.

To further assess significant impacts of an *inter-area interception attack*, we set the attack range to the median NLoS range under the 5-second LocTE TTL setting. As shown in the dotted purple line in Figure 7c, the attacker intercepts almost all packets (**97.9%**) regardless of the short LocTE TTL value.

By changing the inter-vehicle space, we evaluate the attack effectiveness with different traffic densities. We run simulations with inter-vehicle space being 30 (i=30m), 100 (i=100m) and 300 (i=300m) meters. As shown in Figure 7d, the *inter-area interception attack* performs steadily under different road density settings. Specifically, the packet interception rates when inter-vehicle spaces equal to 30m, 100m and 500m are **46.8%**, **47.8%** and **44.7%** respectively.

With the default 30 meters of inter-vehicle space, we find the efficiency of GF algorithm is low on two-direction roads as shown by the blue solid line in Figure 7e. This is because a packet forwarder using GF algorithm will select a vehicle close to its communication range boundary toward the destination. If such a vehicle is heading in an opposite direction against the forwarder, it may move away from forwarder's communication range before receiving the packet, leading to packet loss as we discussed in §III-B. Regardless of GF algorithm's low efficiency, the attacker with the worst NLoS range intercepts **46.8%** of the *vulnerable packets* in single direction scenarios and intercepts **58.3%** of the *vulnerable packets* in two direction scenarios.

Figure 8 shows the accumulated packet interception rates over time in different DSRC scenarios. We name the lines as `'attack range_changed parameter'`. *dflt* means the simulation run uses the default settings. To summarize, an *inter-area interception attacker* with the median LoS range achieves a 100% interception rate. The attack effectiveness decrease as the LocTE lifetime becomes shorter. Road density does not affect the attack effectiveness. The attack is more effective on two direction roads although GF performs poorly in this scenario.

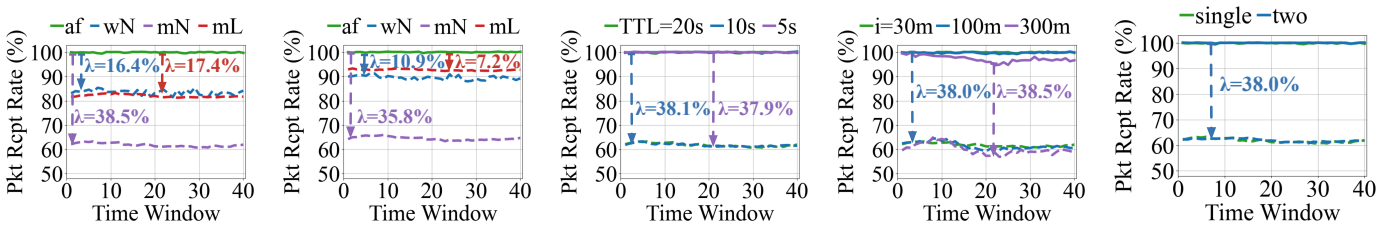
Effectiveness of *intra-area blockage attack*. For the *intra-area blockage attack*, we set the destination area to be the whole 4,000 meters road segment. Every vehicle on the road is a target of the CBF packet sent from a randomly selected vehicle every second. We simulate each setting one hundred times and calculate the packet reception rate as the number of vehicles that received the packet divided by the number of vehicles on the road when the source generates the packet. Similarly, we calculate the packet blockage rate λ as the average packet reception rate drop from attacker-free to attacked scenarios over 40 time bins.

Again, we first evaluate the attack effectiveness with different attack ranges in both DSRC and C-V2X scenarios. The results are shown in Figure 9a and Figure 9b. For reference, we show the packet reception rate of attacker-free (af) scenarios as the green lines in the figures. The packet reception rate is consistent at around 100%. This confirms that the CBF algorithm distributes the packet to all vehicles within the destination area in attacker-free scenarios.

We then set the attack range to the worst NLoS range (wN) and the median NLoS range (mN). We find that the number of received vehicles decreases as the coverage of the attacker increases from the worst NLoS range (blue lines) to the median NLoS range (purple lines) as shown in Figures 9a and 9b. With an attacker with the median NLoS range, the blockage rates λ are **38.5%** and **35.8%** with DSRC and C-V2X, respectively. However, when we increase the attack range to the median LoS range (mL), the number of received vehicles increases as shown by the red lines in the figures. This is because when the attack range is larger than a threshold, the number of first-time receivers of the replayed packet will dominate the number of total receiving vehicles within the packet distribution area. For example, under the median C-V2X LoS range (1,705 m) attack, $(1,705 \times 2)/4,000 \approx 85\%$ of the vehicles on the road segment will receive the replayed packet. We further tune the attack range to find the most effective value. Against both median NLoS range DSRC vehicles (486 meters range) and C-V2X vehicles (593 meters range) with the default simulation settings, we find the 500 meters of attack range to be most effective.

We also analyze the attack effectiveness against different packet source locations. In our simulation, we set the vehicle communication range as the median NLoS range using DSRC (486 meters) and set the attack range to 500 meters. Thus, the *fully covered area* has a length of $(500 - 486) \times 2 = 28$ meters. As a result, the attacker achieves **62.8%** blockage rate against the CBF packets generated inside the *fully covered area* and **37.2%** blockage rate against other packets. The 62.8% blockage rate indicates the packet distribution is blocked along both directions of the road because it is greater than 50%.

We then evaluate the attack effectiveness against different LocTE TTL values. We use DSRC and set up an attacker with the median NLoS range. As shown in Figure 9c, we first find that the CBF algorithm efficiency does not change with different LocTE lifetimes from 5 seconds to 20 seconds. This is because for each hop, vehicles using CBF decide the timing to re-broadcast the packet based on their distance to the last hop. Thus, the LocTE TTL values have no impact on CBF transmission efficiency. Accordingly, the attack effectiveness also does not change with various LocTE TTL values as shown



(a) Attack range (DSRC) (b) Attack range (C-V2X) (c) LocTE TTL value (DSRC) (d) Inter-vehicle space (DSRC) (e) Number of directions (DSRC)

Fig. 9: The effectiveness of *intra-area blockage attack* with different attack ranges (a & b), LocTE TTL values (c), inter-vehicle spaces (d) and the number of directions (e). Solid lines denote the attacker-free scenarios, dashed and dotted lines denote the attacked scenarios. λ indicates the packet blockage rates.

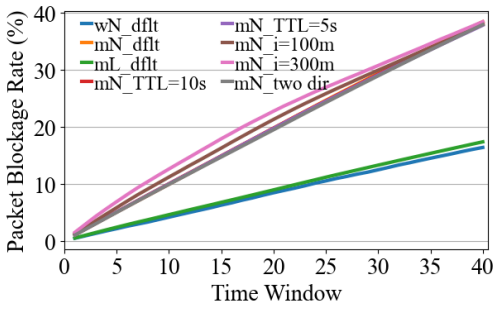
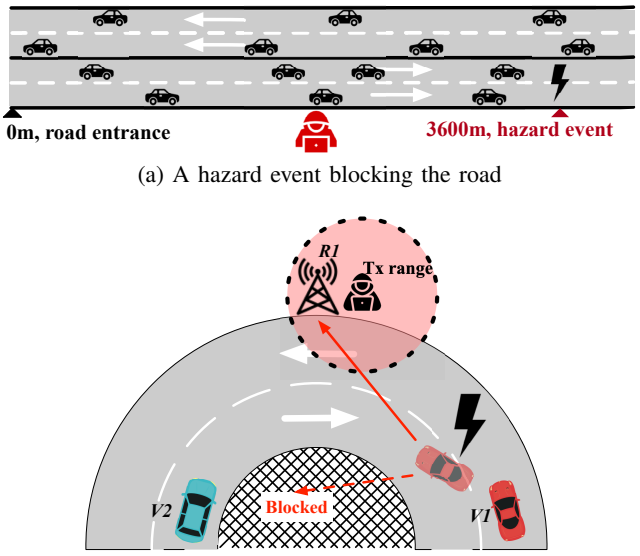


Fig. 10: The overall effectiveness of the *intra-area blockage attack* in different scenarios using DSRC.



(a) A hazard event blocking the road

(b) Illustration of hazard event happened near a sharp turn

Fig. 11: Scenarios that the attacks can be launched to invalid the benefits to traffic efficiency (a) and road safety (b).

in dashed lines in Figure 9c. The blockage rates with 20, 10 and 5 seconds LocTE TTL are **38.5%**, **38.2%** and **37.9%** respectively.

To understand the attack effectiveness on the road with different traffic densities, we insert a median NLoS range attacker into DSRC vehicles and change the value of inter-vehicle space. We increase the inter-vehicle space from the default value of 30 meters to 100 meters and 300 meters. As shown in Figure 9d, the packet blockage rates steadily stay around **38%**.

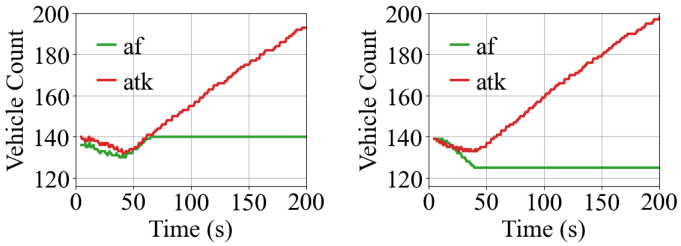
Unlike the GF algorithm, the CBF algorithm efficiency is not impacted by the existence of crossing traffic forwarders since CBF efficiency is not sensitive to their heading directions. The number of vehicles that receive the packet doubles when lanes heading in the opposite direction are added to the road segment as shown in Figure 9e. The blockage rates against traffic on single direction and two directions roads are **38.5%** and **38%**, respectively.

Figure 10 shows the attack effectiveness in various DSRC scenarios. The attack coverage is the only factor impacting the attack effectiveness. Increasing attack range does not always lead to higher blockage rate.

B. Attack Impacts

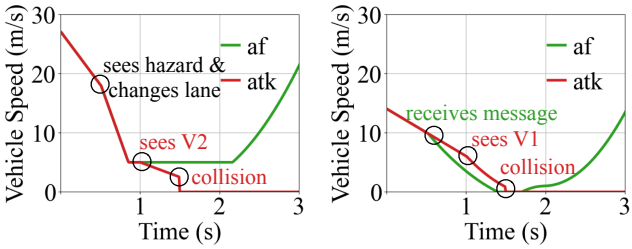
Impacts on traffic efficiency. To assess the attack impacts on traffic efficiency, we consider a showcase scenario shown in Figure 11a. A hazard event blocks both eastbound lanes at the spot 3,600 meters away from the entrance of the 4,000 meters road segment. The eastbound traffic behind the spot (0-3,600 meters) is blocked. The traffic model and other parameters for traffic and communication are the same as the default simulation settings used in §IV-A. We assume the vehicles and the attacker use DSRC. When the event happens at the fifth second of the 200 seconds simulation, we study two cases. In case 1, the heading vehicles facing the hazard event use the GF algorithm to notice the vehicles have not enter the road yet. In case 2, the heading vehicles behind the event use the CBF algorithm to notice all vehicles already on the road and about to enter the road. The attacker launches the *inter-area interception attack* against case 1 and launches the *intra-area blockage attack* against case 2.

Figure 12a shows the number of vehicles on road over time in case 1. We assume the attacker achieves the median NLoS communication range. After the event happens at 5 s, in the attacker-free scenario (af, green line), the packets are



(a) *inter-area interception attack* against the GF algorithm (b) *intra-area blockage attack* against the CBF algorithm

Fig. 12: Number of vehicles on the road in different scenarios. The *inter-area interception attack* and *intra-area blockage attack* cause traffic jams by stopping the transmission of the hazard notification.



(a) Speed profiles of V1 (b) Speed profiles of V2

Fig. 13: Speed profiles of V1 and V2: in the attacked scenario (atk), V2 fails to receive the warning from V1, causing a collision.

received by the vehicles at the entrance after 60 seconds due to the low efficiency of the GF algorithm in two-direction traffic scenarios. From 65 s, the vehicles at the entrance stop entering the blocked road segment and the current on-road vehicle number stays at 140. In the attacked scenario (atk, red line), the attacker blocks the event notification. Without being noticed, the vehicles at the entrance keep entering the road. The number of on-road vehicles increases to 195 at the end of the 200 seconds simulation run, indicating a severe traffic jam.

In case 2, we assume an attacker with 500 meters communication range. In the attacker-free (af) scenario, vehicles behind the entrance immediately receive the notice distributed by the CBF algorithm and choose not to enter the blocked road. Thus, the number of on-road vehicles stops increasing right after 5 s as shown by the green line in Figure 12b. The drop of vehicle number from 5 s to 35 s is due to the exit of the vehicles in front of the event spot (3,600 - 4,000 meters). The number of vehicles stays at 125 after 35 s. In the attacked scenario (atk), the number of vehicles keeps increasing since the notification cannot be distributed to the road entrance. The number of vehicles on road reaches 201 at the end of the 200 seconds simulation as shown by the red line in Figure 12b.

Impacts on road safety. To validate the impacts of *intra-area blockage attack* on road safety, we consider a use scenario shown in Figure 11b, where V1 and V2 are traveling in lanes toward opposite directions. V1 is traveling at a speed of 27 m/s and V2 is traveling at a speed of 14 m/s. While they are approaching the curve, both vehicles decelerate at a rate of 2 m/s^2 as shown by their speed profiles in Figure 13a and 13b. Since the environment (oblique mesh semicircle) blocks the signal transmission between two ends of the curve, a roadside infrastructure R1 is located at the outer edge of the road curve assisting the inter-vehicle communication between the vehicles at the two ends. The attacker locates beside R1 and it can change its transmission power to control its transmission range.

V1 decides to switch to the opposite lane after it identifies an upcoming hazard in front of it. To change the lane, V1 further increases its deceleration to 4 m/s^2 as shown in Figure 13a, it also broadcasts a warning message using CBF to indicate that it is changing lanes. With the assistance of R1, V2 immediately receives the warning and makes a further deceleration as shown in the green line in Figure 13b. In this case, V1 does not collide with V2 and slowly returns to its original lane with a constant speed after passing the hazard spot as shown in the green line in Figure 13a.

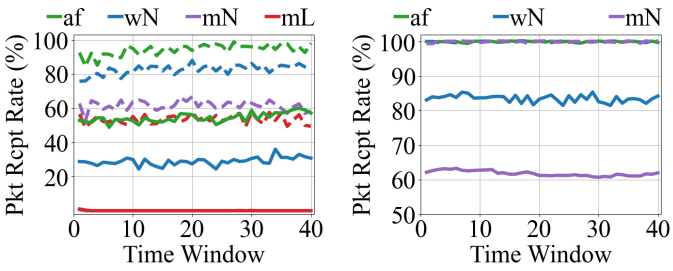
However, the attacker can launch the *intra-area blockage attack* to cause a collision. Upon capturing the warning message from V1, the attacker immediately replays it and makes it only heard by R1 using the variant of the *intra-area blockage attack* introduced in §III-C. In this case, R1 discards the buffered packet and V2 cannot receive the warning for decelerating in advance. Both V1 and V2 make emergency brakings after they see each other, which is too late to avoid a collision.

V. Mitigation

A. Inter-area Interception Attack

To protect vehicular communication against the *inter-area interception attack*, we should eliminate one or more vulnerabilities exploited by the attacker, namely, unencrypted beacons, absence of plausibility checks, and absence of acknowledgment. The mitigation solution should avoid introducing high overhead. Encrypting beacons sent every three seconds introduces non-negligible overhead to both beacon senders and receivers; Using acknowledgment for packet forwarding does not prevent victim vehicles from making wrong forwarding decisions. What is worse is that it reduces communication efficiency when ACKs are lost. As a result, we propose a plausibility check mechanism to mitigate the impact of *inter-area interception attack*.

To perform the plausibility check, the beacon receiver calculates the distance from itself to the position included in the beacon to check whether the source vehicle of the beacon is reachable. When a vehicle receives a packet, it accepts the packet only if the packet sender is reachable according to sender's beacon. To reduce the overhead, our mitigation solution requires vehicles to activate the plausibility check before forwarding packets instead of upon receiving beacons. When a vehicle forwards a packet using the GF algorithm, it finds a neighbor closest to the destination area and activates the plausibility check, it only forwards the packet to that



(a) *inter-area interception attack* (b) *intra-area blockage attack*

Fig. 14: Evaluation results of the mitigation solutions.

neighbor if the distance between itself and the neighbor's position included in the beacon is smaller than a threshold.

To evaluate the effectiveness of the proposed mitigation solution, we implement the solution in the simulator and run simulation of DSRC scenarios. We set the threshold of the plausibility check to the median DSRC NLoS range (i.e., 486m) and simulate with different values of the attack range. For each attack range, we run the simulation 100 times and calculate the packet reception rate of each time bin as in §IV. We show the results in Figure 14a; solid lines present the results without mitigation and dashed lines present results with mitigation. The solution increases the packet reception rate by **53.7%**, **61.6%**, and **53.4%** against the attacker with coverage of the worst NLoS range, median NLoS range, and median LoS range.

Notably, with the plausibility check, the packet reception rates under the worst NLoS range and the median NLoS range attacks (blue and purple dashed lines) are higher than the packet reception rate under the attacker-free scenario without plausibility check (solid green line), which further indicates the necessity of the plausibility check given the highly dynamic topology of connected vehicles. Driven by this observation, we simulate the scenario where plausibility check is used in the attacker-free scenario. The green dashed line shows that the plausibility check increases the packet reception rate to 94.3%, increasing the packet reception rate by 39.9% compared with the no-plausibility check case.

B. Intra-area Blockage Attack

A straightforward solution to mitigate the impact of the *intra-area blockage attack* is to include the RHL field in the integrity-protected payload of the CBF packet. However, this solution requires the change of CBF packet structure, making it incompatible with the current standard. Instead, we propose an RHL check based solution.

As discussed in §III-C, the attacker has to intercept the packet from the source (i.e., hop zero) before the packet is spread out to make the attack effective. The key observation is that the RHL value of the packet when it is broadcast from the source is always large (e.g., RHL = 10) to ensure the packet can pass enough hops before every vehicle in the destination area receives it. On the other hand, the attacker needs to decrease the RHL value to 1 to ensure that new packet receiver (i.e., hop two) vehicles discard the packet instead of buffering it. Thus, the hop one vehicles will observe a steep drop of the RHL value (e.g., from 10 to 1) in the duplicated packet comparing the RHL values of the packets received from hop zero and the attacker. Based on the above insight, in our proposed solution, we set the RHL drop smaller than a threshold of 3 to make a duplicated packet acceptable. Once a hop-one vehicle receives a packet for the second time but with an RHL value drop larger than 3, the vehicle does not refer to it as a duplicated packet and does not discard the packet it is buffering.

To evaluate the effectiveness of our proposed solution, we implement the RHL value check on top of the CBF implementation in our simulator with the RHL threshold set to 3. We run DSRC simulations with the worst NLoS range attacker and the median NLoS range attacker 100 times each and plot the packet reception rates in Figure 14b. The packet reception rates in the attacked scenarios are plotted in solid lines and the dashed lines show the results of mitigated scenarios. As shown, the RHL check eliminates the negative impacts caused by the *intra-area blockage attack* and the packet reception rates align with the results in attacker-free scenarios.

VI. Related Work

Security of geographic routing for connected vehicles. Recent years have witnessed several security studies on geographic routing protocols for connected vehicles or vehicular ad hoc networks (VANETs) [20]–[23]. Celes et al. proposed to secure geographic routing with an authentication mechanism based on a majority vote approach that requires nodes to exchange their LocTs with their neighbors frequently [20]. Francis et al. proposed a trust-based geographic routing which establishes a trust-based secure communication by calculating the trust value of all nodes based on location trusted information and direct trusted information between the sender and the destination node [21]. Shokrollahi et al. further extended the trust-based geographic routing protocol by leveraging distance prediction and packet monitoring to update the recommendation trust about the next-hop [23]. Benguenane et al. focused on detecting malicious nodes in geographic routing among connected vehicles and proposed a collaborative approach that disseminates the detected attackers using beacons with the attacker's address [22]. The above studies all are centered on the solutions to secure geographic routing but none of them is compatible with standard geographic routing protocols. Different from them, we investigate insecurity implications of GeoNetworking, a standard geographic routing protocol for connected vehicles; We uncover real attacks against inter-area and intra-area forwarding algorithms that are adopted by GeoNetworking and will likely be used for the upcoming connected vehicles; We propose the mitigation solutions to the proof-of-concept attacks.

Security of ad-hoc network routing. Securing geographic routing protocols can be traced back to ad-hoc network routing security, which has been actively studied in the literature for a long time. On the attack front, our proposed *inter-area*

interception attack is most similar to the blackhole attack [7], which is one DoS attack against ad hoc network routing. In a blackhole attack, the attacker claims to have the shortest path to the destination area via forged beacons. Once it receives the packet, it stealthily drops the packet to cause DoS. However, the blackhole attack requires the attacker to forge and advertise fake beacons to its neighbors, which is only feasible for an attacker with a certificate since the authentication of beacons is required by GeoNetworking. On the defense front, [24] proposed cross checking to identify cooperative black holes and [25] developed a lightweight detection scheme. However, none of the above defense solutions are effective because the *inter-area interception attack* only relays beacons from legitimate nodes; Detecting malicious nodes is of little help. The second attack in our work, i.e., the *intra-area blockage attack*, to the best of our knowledge, has not been studied in the existing ad-hoc network routing attacks as they need to block the distribution of packets via flooding-based algorithms (e.g., CBF algorithm).

Access layer attacks against connected vehicles. In addition to routing attacks, there exist other access layer attacks against connected vehicles. Twardokus et al. proposed a DSRC jamming attack [15]. By knowing the victim's pseudonym used for hiding the vehicle's permanent ID, the attacker sniffs for the basic safety message (BSM) period and transmits a jamming signal within every BSM interval. They later devised two DoS attacks against C-V2X in 4G and 5G networks [16]. These two attacks exploit vulnerabilities in the Semi-persistent Scheduling Algorithm of the C-V2X physical layer. In the first attack, by predicting the sidelink resource grids the victim will use, the attacker injects sidelink control information (SCI) to make the victim's basic safety messages transmitted in the same resource grid not recoverable. In the second attack, the attacker transmits in different time-frequency resources so that the victim vehicle which is listening for unoccupied resources cannot find the resource for transmission. The access layer attacks mentioned above target a single victim vehicle while our attacks are launched against multiple vehicles.

Application layer attacks against connected vehicles. There are a number of studies on application-level attacks and mitigations. We briefly introduce two representative studies for a glimpse of emerging risks and possible solutions. Abdo et al. reported platooning application attacks by exploiting vulnerabilities of cooperative adaptive cruise control for connected vehicles [26]. In this work, the attacker has the control of a malicious vehicle with the certificate to sign outgoing packets to the victim vehicles in the platoons and the attacker exploits application layer vulnerabilities to force a platoon to stop, to force two platoons to merge, or to take control of a platoon. Hu et al. further developed an approach to discovering vulnerabilities in the platooning protocols [27]. They proposed a security analysis based on model checking and uncovered attacks that can maliciously split a platoon, lead a platoon to a hazardous situation, or forge wrong platoon depth information to the platoon leader. In this work, we focus on attacks against geographic routing, not the applications enabled. Moreover, we consider outsider attacks which do not need compromised or malicious vehicles.

VII. Conclusion

In this paper, we present two proof-of-concept attacks against the GeoNetworking protocol, a standard geographic routing protocol which was recently released for upcoming rollout of connected vehicles. These two attacks are complementary to block inter-area and intra-area communication. The *Inter-area Interception Attack* exploits vulnerabilities in the Greedy Forwarding algorithm which is used to transmit packets between vehicles from one geographic area to another. The *Intra-area Blockage Attack* leverages vulnerabilities in the Contention-Based Forwarding algorithm which is designed to disseminate packets within a geographic area. Both algorithms are the standardized forwarding algorithms for geographic routing of connected vehicles. However, we find that both algorithms can be exploited for the interception attacks, where the attacker does not need a certificate to get involved in the communication between vehicles and launch the attacks as an outsider statically on the roadside. We have evaluated the effectiveness and damages of these attacks under a variety of traffic and communication settings. We have further discussed the mitigation approaches and validated their effectiveness.

A surprising lesson is that vulnerabilities and attacks are not unknown to the community, as geographic routing security has been extensively studied in different forms in the literature. However, these known risks and lessons do not seem to be prudently taken into account in the standard making, which exposes connected vehicles to similar and simple attacks. Drive safety is paramount for intelligent transportation systems, so security must be treated as first citizen. More efforts from researchers and engineers are warranted and will be rewarding.

Acknowledgements. We are grateful to all anonymous reviewers for their constructive comments. This material is based upon work partially supported by National Science Foundation under grants CNS-1750953, CNS-2112471 and CNS-2246051. Any opinions, findings and conclusions or recommendations expressed in this material do not necessarily reflect the views of the National Science Foundation.

References

[1] 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.

[2] A. Srivastava, A. Prakash, and R. Tripathi, "Location based Routing Protocols in VANET: Issues and Existing Solutions," *Vehicular Communications*, vol. 23, 2020.

[3] "ETSI EN 302 636-4-1: 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," Jan 2020, v1.4.1.

[4] "IEEE 1609.3-2020: IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Networking Services," March 2021.

[5] "ETSI TS 102 731: Intelligent Transport Systems (ITS); Security; Security Services and Architecture," September 2010, v1.1.1.

[6] "IEEE 1609.2.1-2022: IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities," March 2022.

[7] M. Karthigha, L. Latha, and K. Sripriyan, "A comprehensive survey of routing attacks in wireless mobile ad hoc networks," in *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 396–402.

[8] "Maryland Department of Transportation," https://www.roads.maryland.gov/Traffic_Volume_Maps/Traffic_Volume_Maps.pdf, accessed: 2023-02-22.

[9] "Intelligent Driver Model," https://en.wikipedia.org/wiki/Intelligent_driver_model, accessed: 2023-02-22.

[10] "ASTM E2213-03: Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications," Jan 2010, v3.

[11] "ETSI EN 303 613: Intelligent Transport Systems (ITS); LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band," Jan 2020, v1.1.1.

[12] "ETSI EN 302 636-1: Intelligent Transport Systems (ITS). Vehicular Communications. GeoNetworking. Part 1: Requirements," April 2014, v1.2.1.

[13] "New York Department of Transportation," https://www.dot.ny.gov/tdv, accessed: 2023-02-22.

[14] C. Harsch, A. Festag, and P. Papadimitratos, "Secure position-based routing for VANETs," in *2007 IEEE 66th Vehicular Technology Conference*. IEEE, 2007, pp. 26–30.

[15] G. Twardokus, J. Ponicki, S. Baker, P. Carenzo, H. Rahbari, and S. Mishra, "Targeted discreditation attack against trust management in connected vehicles," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[16] G. Twardokus and H. Rahbari, "Vehicle-to-Nothing? Securing C-V2X Against Protocol-Aware DoS Attacks," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. IEEE, 2022, pp. 1629–1638.

[17] "Vehicular AdHoc Networks Simulation," https://github.com/JianshanZhou/Vehicular_AdHoc_Networks_Simulation.git, accessed: 2023-02-22.

[18] Z. Zhong, L. Cordova, M. Halverson, and B. Leonard, "Field Tests On DSRC And C-V2X Range Of Reception," *Utah Department of Transportation5*, 2021.

[19] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in VANET," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 275–285, 2011.

[20] A. A. Celes and N. E. Elizabeth, "Verification based authentication scheme for bogus attacks in VANETs for secure communication," in *2018 International Conference on Communication and Signal Processing (ICCSP)*, 2018, pp. 0388–0392.

[21] F. H. Shajin and P. Rajesh, "Trusted secure geographic routing protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol," *International Journal of Pervasive Computing and Communications*, 2020.

[22] M. Benguenane, A. Korichi, and N. Azzaoui, "Geographical Routing Protocols in VANets: Performance and Security Analysis," in *2nd International Conference on Industry 4.0 and Artificial Intelligence (ICIAI 2021)*, 2022, pp. 158–163.

[23] S. Shokrollahi and M. Dehghan, "Tgrv: A trust-based geographic routing protocol for vanets," *Ad Hoc Networks*, vol. 140, p. 103062, 2023.

[24] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. E. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks." in *International conference on wireless networks*, vol. 2003, 2003, pp. 570–575.

[25] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight sybil attack detection in manets," *IEEE systems journal*, vol. 7, no. 2, pp. 236–248, 2012.

[26] A. Abdo, S. M. B. Malek, Z. Qian, Q. Zhu, M. Barth, and N. Abu-Ghazaleh, "Application level attacks on connected vehicle protocols," in *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*, 2019, pp. 459–471.

[27] S. Hu, Q. A. Chen, J. Sun, Y. Feng, Z. M. Mao, and H. X. Liu, "Automated Discovery of {Denial-of-Service} Vulnerabilities in Connected Vehicle Protocols," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 3219–3236.