perplexity

Additional Problem Statements: DDoS Attacks on 5G-V2X Networks

The integration of 5G technology with Vehicle-to-Everything (V2X) communication expands both capability and attack surface, making DDoS detection and mitigation especially complex. Below are research-driven problem statements addressing the multi-faceted challenge of DDoS attacks in 5G-V2X, reflecting diverse architectures, protocol vulnerabilities, and deployment models.

1. Detection of Stealthy PHY/MAC-Layer DDoS in 5G Sidelink (C-V2X/NR-V2X)

- *Problem*: 5G-V2X systems employing sidelink (PC5) direct communications are vulnerable to targeted jamming and resource exhaustion at the physical and MAC layers. Adversaries can exploit scheduling algorithms and physical-layer signaling to inject low-rate but highly effective DDoS attacks that mimic natural network noise, severely degrading packet delivery ratios among vehicles.
- *Need*: Develop lightweight, real-time monitoring techniques to identify abnormal patterns in sidelink resource usage and distinguish attack-induced packet loss from normal vehicular communication errors[1].

2. DDoS Detection and Mitigation in Multi-Slice 5G-V2X Networks

- *Problem*: Network slicing in 5G enables multiple logical V2X networks to coexist on shared infrastructure, but attackers can exploit inter-slice (across slices) and intra-slice (within slice) vulnerabilities. Coordinated DDoS attacks may originate from multiple slices, overwhelming shared or isolated resources and evading slice-level IDS solutions.
- *Need*: Design scalable, federated intrusion detection frameworks that collaboratively detect and trace attacks spanning multiple slices while minimizing cross-slice privacy and isolation breaches[2] [3] [4].

3. Adaptive DDoS Defense in 5G-Enabled Mobile Edge Computing (MEC) for V2X

- *Problem*: 5G-V2X leverages MEC for low-latency processing, but MEC servers become attractive DDoS targets. The high bandwidth and device density of 5G can allow attackers to overload edge resources quickly, disrupting safety-critical V2X services at the source.
- *Need*: Develop adaptive, AI-driven IDS capable of detecting rapid traffic surges and novel attack signatures at the edge, without overburdening MEC resources or introducing new bottlenecks[5] [6].

4. Detection of DDoS-Driven Service Starvation in V2X Broadcasting and Multicasting

- *Problem*: Vehicles often rely on periodic broadcast of safety messages. DDoS attacks can exploit high-frequency broadcasting requirements in 5G-V2X, causing service starvation or message suppression—potentially triggering accidents or disrupting traffic control.
- *Need*: Create detection methods that differentiate between legitimate network congestion (e.g., rush-hour broadcasts, emergency alerts) and malicious, coordinated traffic floods targeting V2X broadcast/multicast services[7] [1].

5. Privacy-Preserving Intrusion Detection Against DDoS in 5G-V2X

- *Problem*: Real-time detection of DDoS attacks often requires monitoring sensitive vehicle data and communication patterns. Privacy concerns make widespread sharing and analysis of raw network data infeasible.
- *Need*: Design privacy-preserving, self-supervised or federated intrusion detection systems that ensure timely DDoS detection without compromising personal or operational data privacy[6].

6. Resilience Against Resource Exhaustion via Cross-Domain DDoS in V2X

- *Problem*: Given the reliance on multiple domains (cellular core, edge, vehicular ad-hoc), cross-domain DDoS attacks orchestrate simultaneous overloads at various points—e.g., core network, access network, and direct sidelink—making single-point detection insufficient.
- *Need*: Engineer cross-layer, multi-domain detection and response mechanisms, leveraging both local (vehicle, MEC) and global (core, cloud) intelligence to enable distributed defense and automatic response coordination[8] [9].

7. AI/ML-Driven DDoS Detection Robust to High-Speed and Dynamic Topologies

- *Problem*: 5G-V2X environments are distinguished by ultra-low latency, high mobility, and constantly shifting network topology. Existing IDS approaches may falter as traffic baselines and device memberships change rapidly, increasing false positives or missing transient, high-impact DDoS events.
- *Need*: Advance AI/ML anomaly detection models capable of real-time adaptation to traffic variability, topology changes, and new network slices—without sacrificing detection accuracy or warning delay[10] [3].

These problem statements highlight the urgent need for **architecture-aware, adaptive, and privacy-preserving DDoS detection technologies** for 5G-V2X. They capture emerging challenges at the intersection of new 5G features (sidelink, network slicing, MEC) and the unique requirements of vehicular communications. Each points to current gaps actively targeted by state-of-the-art research in the field[1] [2] [3].

⁂

1. https://www.rit.edu/wisplab/sites/rit.edu.wisplab/files/2023-03/Towards_Protecting_5G_Sidelink_Scheduling_in_C_V2X_Against_Intelligent_DoS_Attacks.pdf
2. https://orbilu.uni.lu/bitstream/10993/54376/1/[Camera_Ready]Federated_learning_based_inter_slice_Attack_Detection_for_5G_V2X_Slicing_networks.pdf
3. https://orbilu.uni.lu/bitstream/10993/53010/1/_Final_CameraReady__Deep_Learning_based_Intra_slice_Attack_Detection_for_5G_V2X_Sliced_Networks.pdf
4. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/cmu2.12778
5. https://arxiv.org/pdf/2202.00005.pdf
6. https://www.sciencedirect.com/science/article/pii/S1570870524002853
7. https://www.sciencedirect.com/science/article/pii/S2590005621000321
8. https://ijariie.com/AdminUploadPdf/EXPLORING_5G__CHALLENGES_AND_SECURITY_ISSUES_IN_CELLULAR_TECHNOLOGIES_ijariie24709.pdf
9. https://www.itm-conferences.org/articles/itmconf/pdf/2022/03/itmconf_icaie2022_01025.pdf
10. https://www.nature.com/articles/s41598-024-82313-x