perplexity

Technical Problem Statements in DDoS Vulnerabilities of V2G Systems

1. **Resource-Constrained Real-Time DDoS Detection**
   V2G endpoints (charging stations EV on-board units) and grid controllers often have limited CPU, memory, and bandwidth. Designing intrusion-detection systems (IDS) capable of accurately identifying high-volume, multi-vector DDoS traffic in real time—without degrading normal V2G communication performance—remains an open challenge[1].
2. **Protocol-Specific Flooding Exploits (ISO 15118 & OCPP)**
   Attackers can overwhelm V2G's bidirectional communication protocols (ISO 15118, OCPP) by initiating excessive session negotiations or malformed control messages. Characterizing these protocol-level flood patterns and defining fine-grained detection rules that avoid false positives on legitimate grid services is still unresolved[2].
3. **Botnet Coordination via Compromised EVCS**
   Compromised EV charging stations can be used as botnet nodes to launch synchronized DDoS against central aggregators or grid interfaces. Formulating methods to fingerprint charging-station traffic for early botnet membership identification—and isolating malicious stations without disrupting normal charging—is a critical unsolved problem[2].
4. **Amplification Attack Mitigation in V2G Context**
   Publicly accessible grid services integrated into V2G (e.g., DNS, NTP) enable reflection/amplification DDoS. Quantifying amplification factors specific to V2G deployments and deploying effective rate-limiting or response-scrubbing mechanisms tailored to EV load profiles are still in nascent stages of research.
5. **Authentication-Server Flood Protection**
   V2G authentication servers validate millions of charge/discharge transactions. Attackers may saturate these servers with fake credential requests, blocking legitimate EV access. Defining lightweight challenge-response protocols that differentiate genuine EVs from bots—while maintaining compatibility with existing PKI infrastructures—remains an open design problem.
6. **Adaptive Defense under Dynamic Grid Loads**
   The variable demand/supply characteristics of V2G services cause normal traffic patterns to change rapidly. IDS that adapt threshold-based DDoS detection to shifting baselines without human intervention have yet to achieve robust performance across diverse grid conditions.
7. **Integrated Multi-Layer DDoS Forensics and Recovery**
   Beyond detection, V2G operators need automated forensics to trace attack provenance across EVCS, network segments, and central controllers. Designing cross-layer logging and correlation frameworks—capable of reconstructing DDoS campaigns for post-mortem analysis and system recovery—constitutes an under-researched area.

8. **Scalable Anomaly Detection with Low False Positives**
   Machine-learning models (e.g., CNNs, bio-inspired classifiers) show high detection accuracy in simulations but often yield unacceptable false-positive rates in real deployments. Achieving scalable anomaly detection that maintains precision and recall at grid-scale loads remains a pressing challenge[1].
9. **Physical and Cyber Covert DDoS Attacks**
   Attackers with physical access (e.g., to EVSE USB ports) can deploy malware that coordinates DDoS while masking from network traffic monitors. Developing unified security models that consider both physical compromise and network-level DDoS detection is still an open research question.
10. **Granular Rate-Limiting without Service Degradation**
    Traditional rate-limiting may throttle legitimate V2G signaling during peak demand. Crafting adaptive rate-limiting algorithms that protect against volumetric floods yet preserve quality of service for critical grid services (e.g., frequency regulation) remains unsolved.

These problem statements identify core technical challenges for securing V2G systems against DDoS threats, highlighting gaps in detection, protocol resilience, botnet mitigation, adaptive defense, and integrated recovery.

⁂

1. https://scientiairanica.sharif.edu/article_23664_39466754746fda04bd9f9118289f89a5.pdf
2. https://journals.sagescience.org/index.php/jamm/article/download/78/74/96