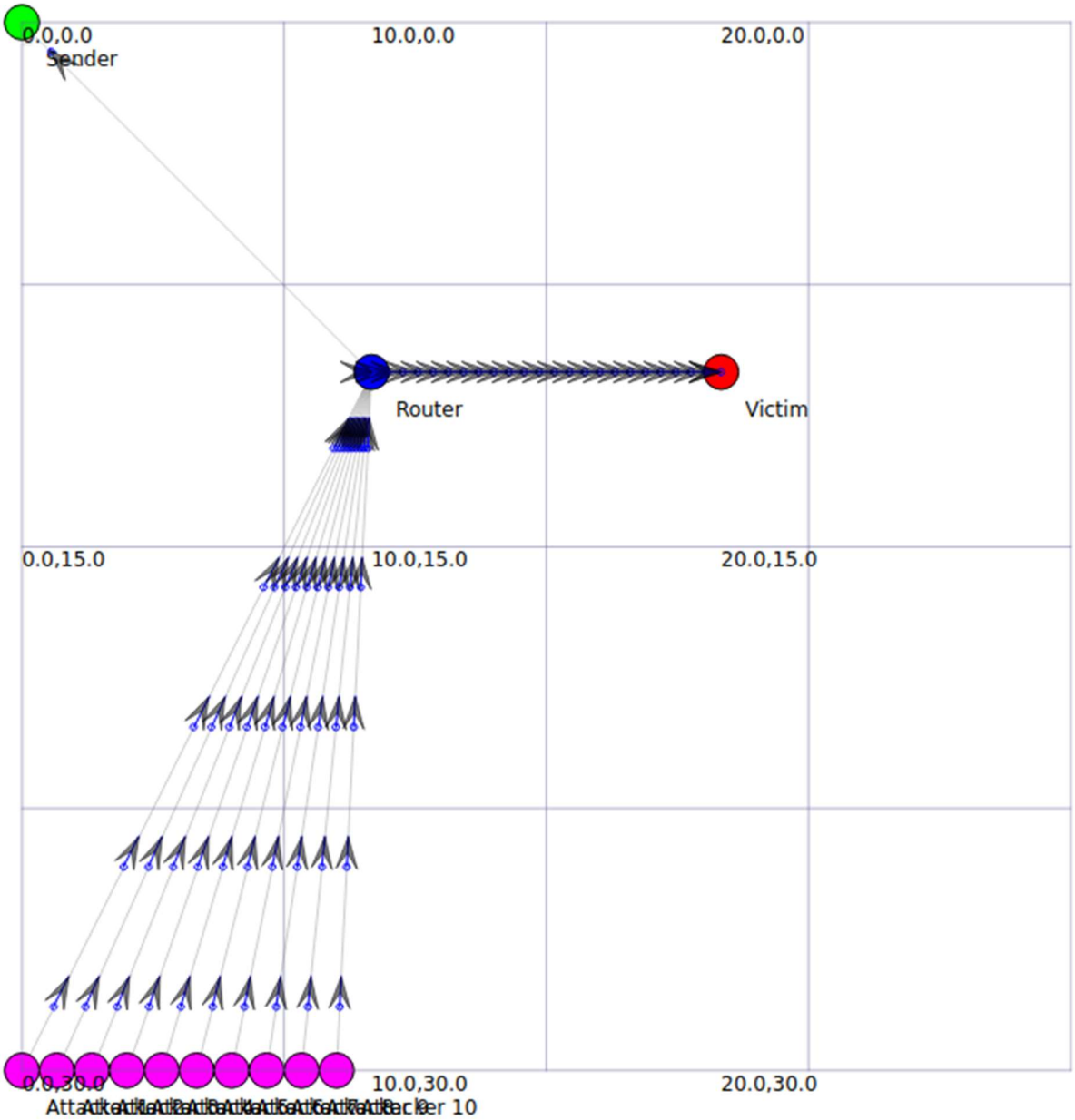
VANET Misbehaviors and Their Functionalities

Blackhole Attack

- Malicious node advertises itself as having the shortest path to the destination.
- Attracts network traffic away from legitimate routes.
- Once traffic is received, packets are dropped instead of forwarded.
- Simulation: Blackhole 1 advertises false route and drops packets.

Distributed Denial of Service (DDoS) Attack

- Multiple attacker nodes (bots) flood the victim with high traffic.
- Overwhelms victim's resources, blocking legitimate communication.
- Simulation: Bots send UDP packets at high rate to victim, degrading TCP traffic performance.

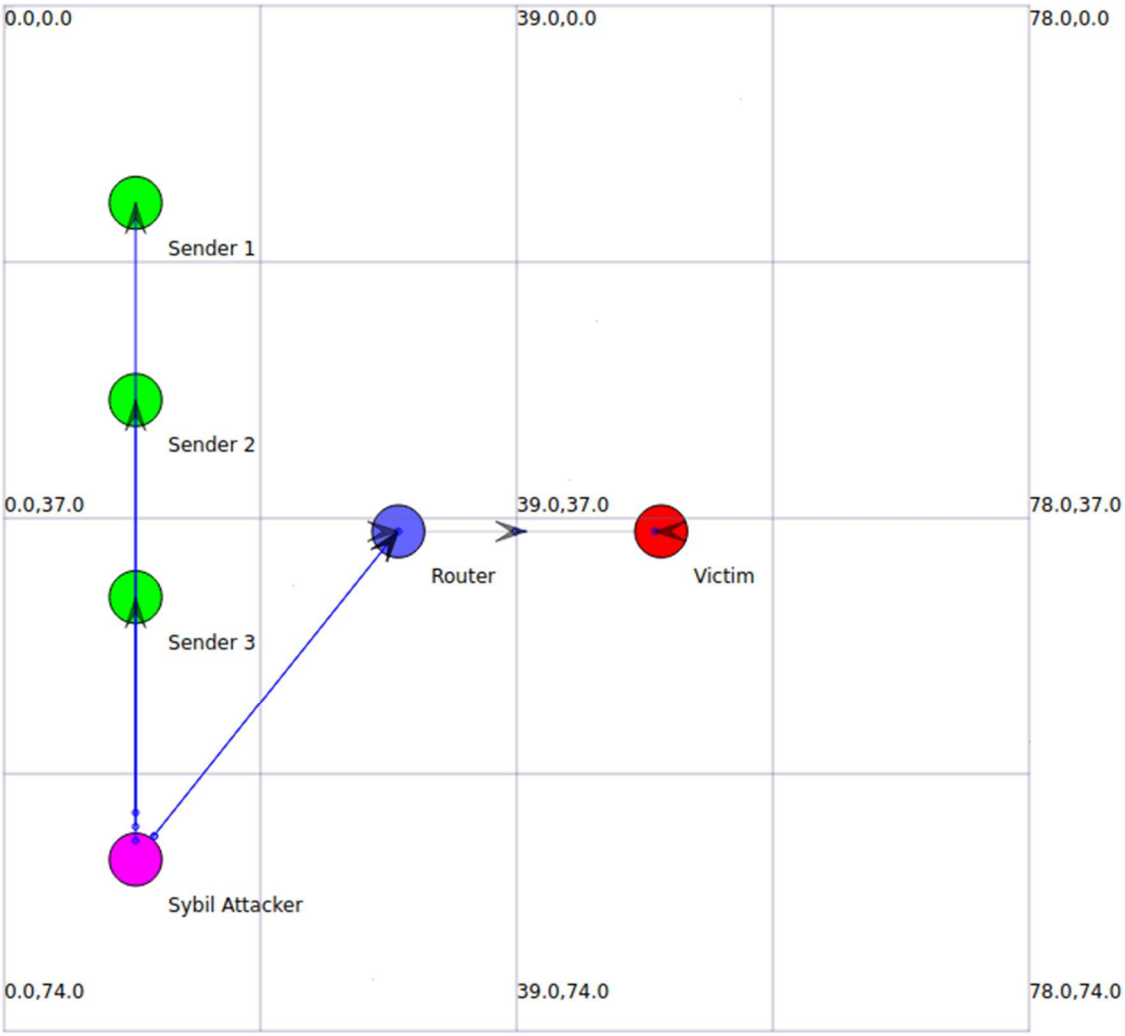


Man-in-the-Middle (MITM) Attack

- Attacker places itself between sender and victim.
- Intercepts, logs, modifies, drops, or forwards packets.
- Simulation: MITM drops packets randomly and modifies others before forwarding.

Sybil Attack

- A single malicious node creates multiple fake identities (Sybil identities).
- Gains disproportionate influence in the network.
- Disrupts routing and communication of legitimate nodes.
- Simulation: Attacker generates multiple Sybil identities sending UDP traffic to victim, overwhelming it.



Wormhole Attack

- Two colluding malicious nodes form a low-latency tunnel between distant network points.
- Tunnel path appears shorter than legitimate routes, attracting traffic.
- Disrupts normal multi-hop routing and compromises network integrity.
- Simulation: Wormhole nodes W1 and W2 create a shortcut, bypassing legitimate routers.