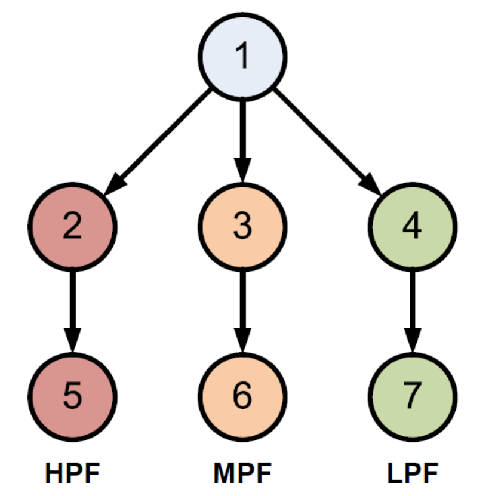
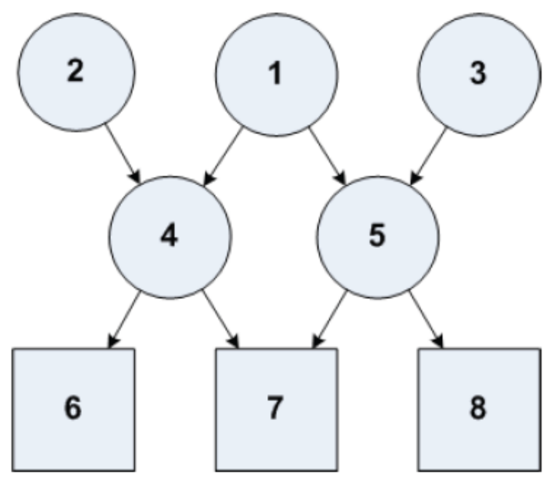
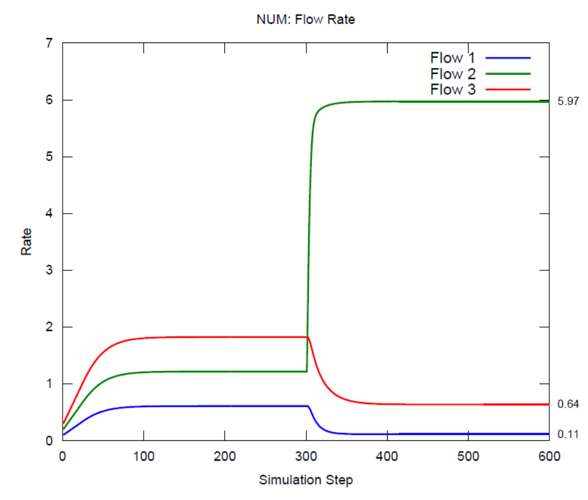
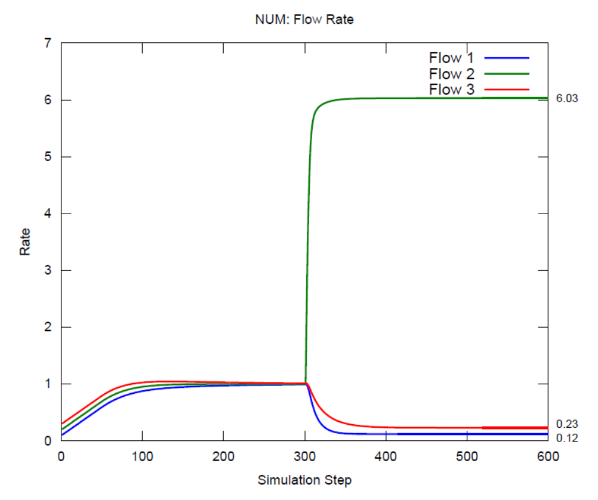
Network Resource Manipulation and Security Concerns of NUM Networks

James Edwards, Scott Rager, Thomas La Porta



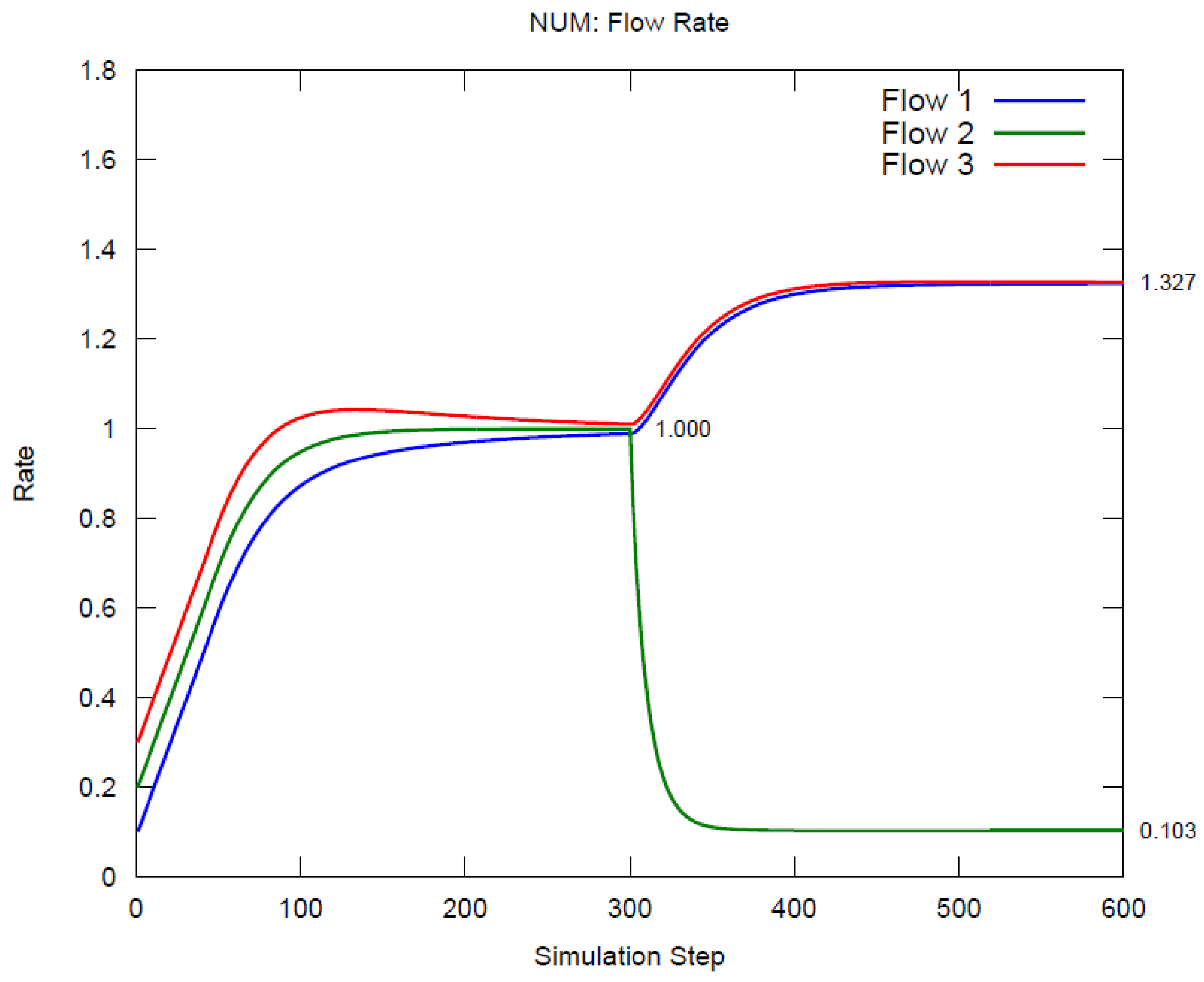


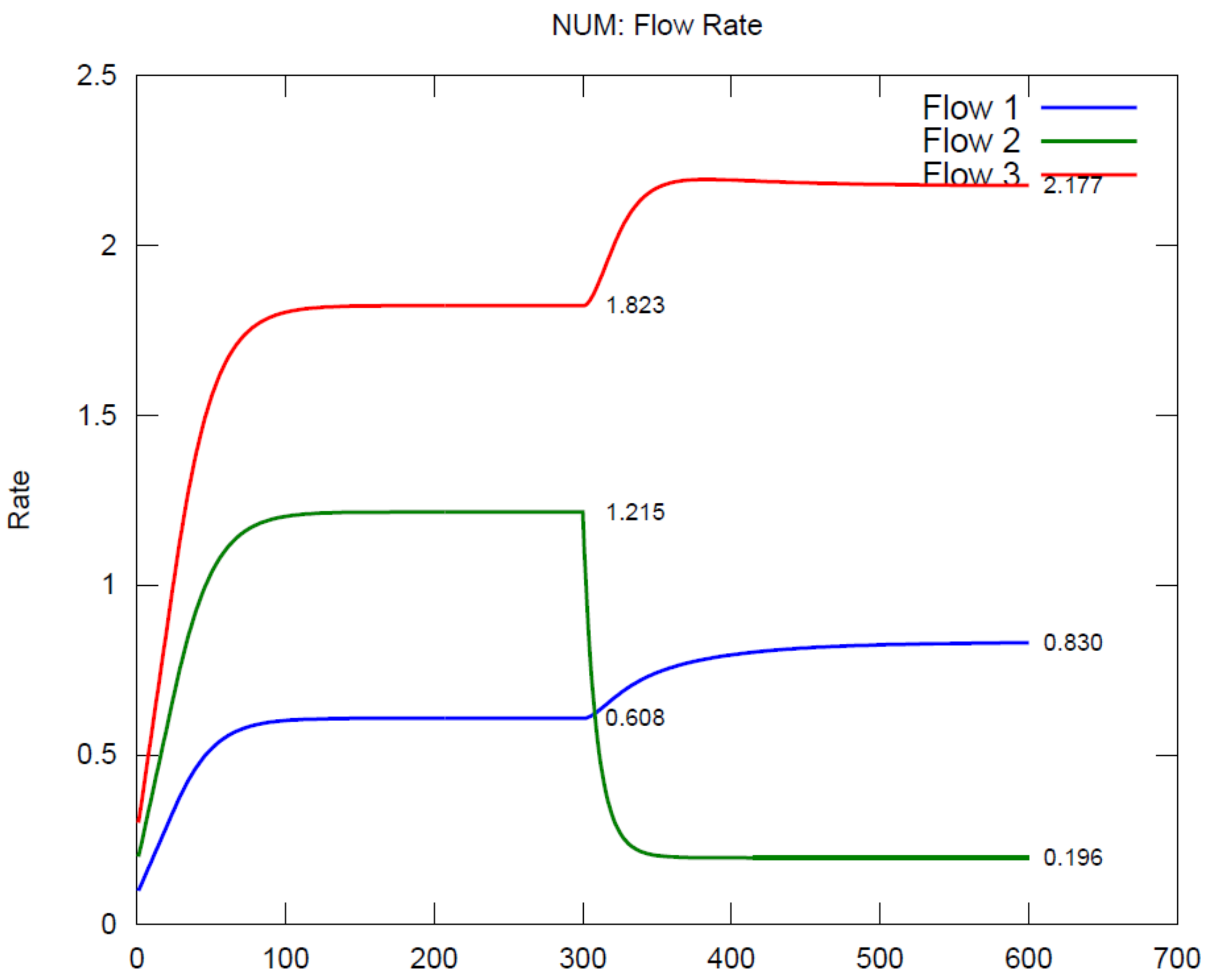




Attack Description and Effects of Misrepresentation

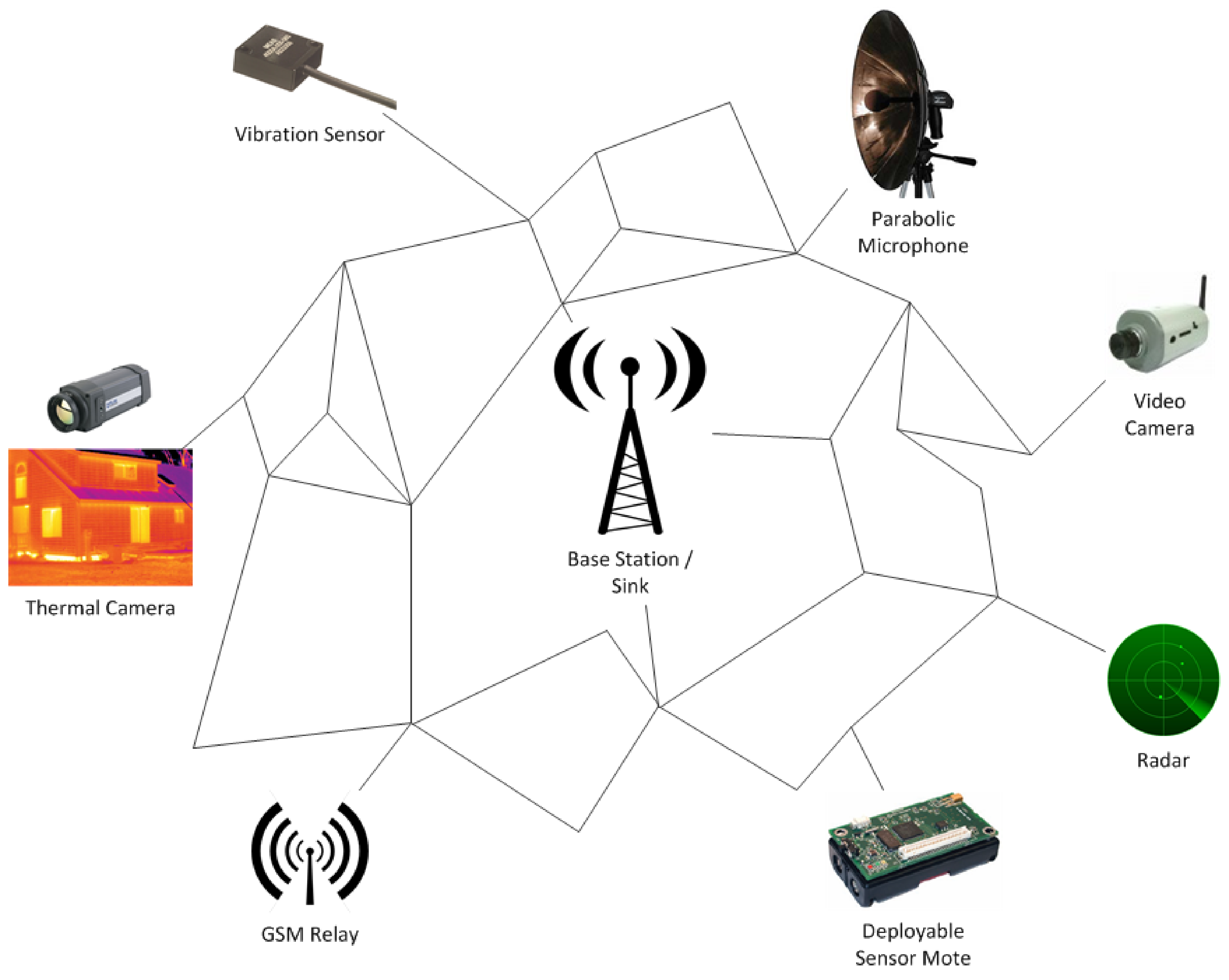
- NUM protocols rely on end-to-end messaging to convey network state and facilitate convergence
- It is necessary that in-flow nodes are able to read and update these control packets
- Attackers lie about their link state, or the link state of others.
- Unlike jamming or selective-forwarding attacks, these attacks simply cause what could be a very real network state, making detection difficult
- We have demonstrated that a single bad actor can devastate a NUM-based network in a variety of ways



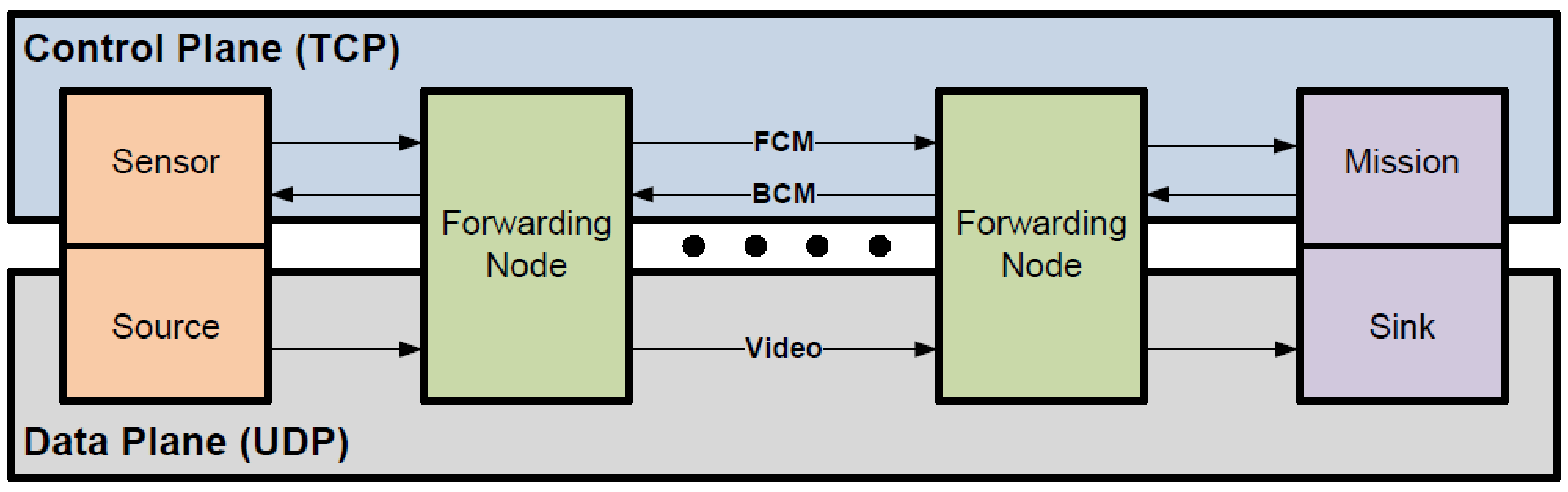


Attacks

- Attackers can:
  - Starve targetted flows for the purpose of achieving a degradation or denial of service
  - Manipulate the network resources such that their own traffic, or that of a conspirator, is prioritized or otherwise treated favorably
  - Influence routing protocols to facilitate other attacks (e.g. man-in-the-middle, selective forwarding, etc)
  - Intentionally overload nodes in order to deplete their energy stores and partition the network into disconnected subgraphs
  - Misrepresent downstream congestion such that compression algorithms are triggered and the quality of transmitted data is proactively degraded



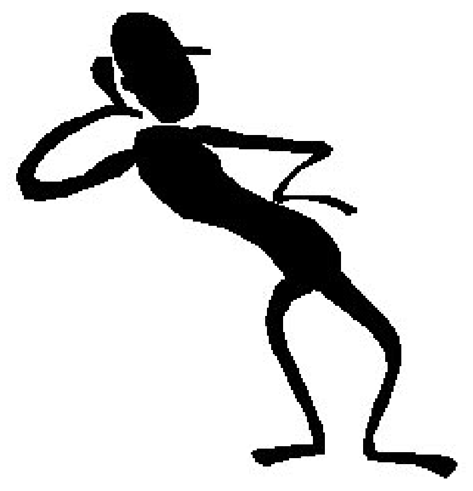
Architecture and Countermeasures



- Control Plane involves control messages in both directions, upstream and downstream
- **Forward Control Message** - Upstream: Conveys interference / congestion information, willingness to pay, marginal utility, power information, etc.
- **Backwards Control Message** - Downstream: Conveys rate information, compression / fusion information.

Possible Countermeasures:

- Implement a HMAC scheme on control messages
  - Ensures data integrity (not corrupted) and authenticity (is from who it claims to be from)
- Implement a Public-Key Infrastructure scheme:
  - Ensures data integrity, authentication and confidentiality
- Probabalistic Eavesdropping
  - An attempt to discover and locate bad actors
- Other countermeasures
  - Hash chain verification – light weight token-based verification
  - Define upper bounds – establish limits for reporting metrics
  - Active link probing – obtain verification of link state through alternative methods.



SPONSORED BY THE US-ARL INTERNATIONAL TECHNOLOGY ALLIANCE