

# Wireless Network Security and Privacy

Autumn 2023

Xiaoyu Ji

Wireless Transport Security

# Agenda

- Fun issues at the wireless transport layer
- Transport-oriented attacks

# Transport Layer

- Transport layer is responsible for **managing end-to-end content delivery**
  - Connection-oriented communication
  - Reliability
  - **Flow control**
  - **Congestion avoidance**
  - **Multiplexing**
  - Ordered delivery
- What do you think of transport?
  - TCP
  - UDP
  - .....

# Wireless Multihop Transport

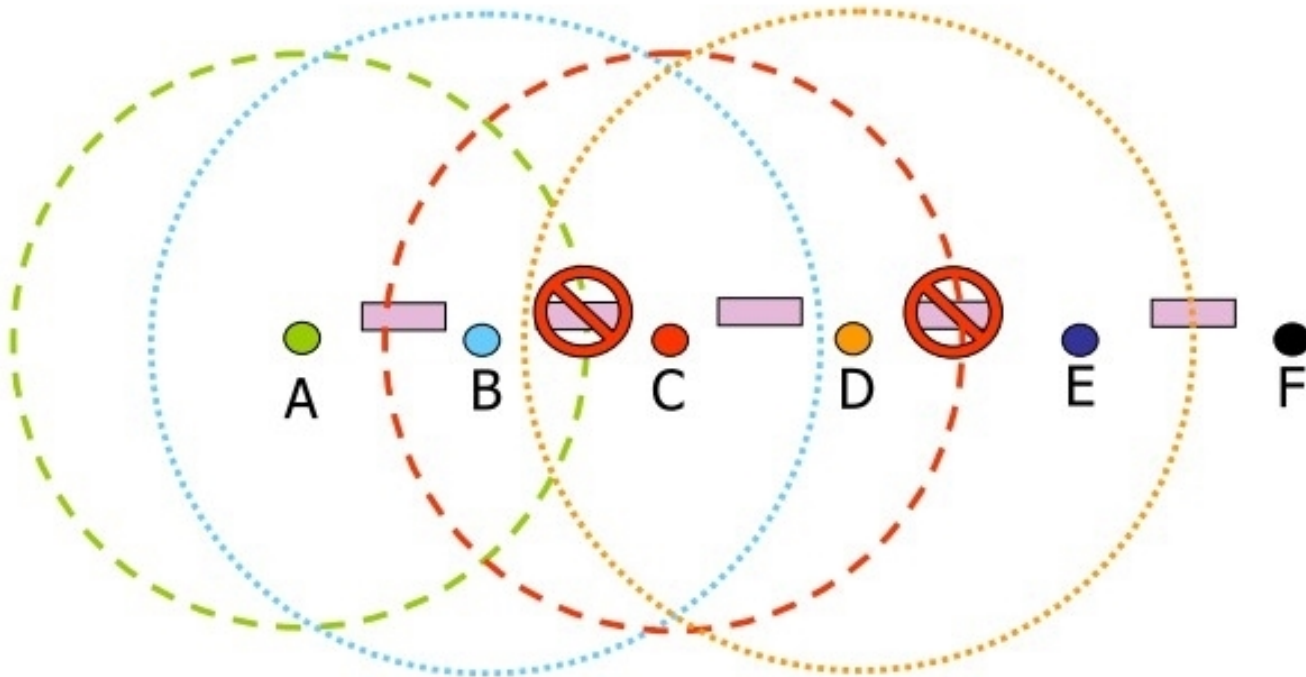
- Transport performance is affected by all protocols living below it
  - Physical layer
    - Errors can be misinterpreted by transport mechanisms: one of the big reasons TCP has difficulties in wireless
  - MAC
    - No collision detection → Transport flows suffer from inter- and intra-flow contention
  - Network layer
    - Transport sessions live only as long as routing paths; path maintenance → session maintenance
    - Mobility: path disconnection/loss causes different behaviors in different routing protocols, all of which affect transport

# Phy → Transport Impact

- TCP interprets errors and tries to mitigate their effects using congestion control
  - CSMA/CA vs. CSMA/CD
  - But, it usually can't distinguish congestion loss from transmission errors
  - Congestion control may be invoked when not needed
  - TCP + transmission errors → reduced throughput

# MAC → Transport Impact

- More hops/path means more medium usage
  - Increased competition for medium, even among nodes in the same routing path
  - Higher interference and hidden/exposed terminals



# Mobility → Transport Impact

- Node mobility leads to route changes
  - Route can fail, data lost on old route, new route formed, **TCP timeout starts data on new path**, over and over

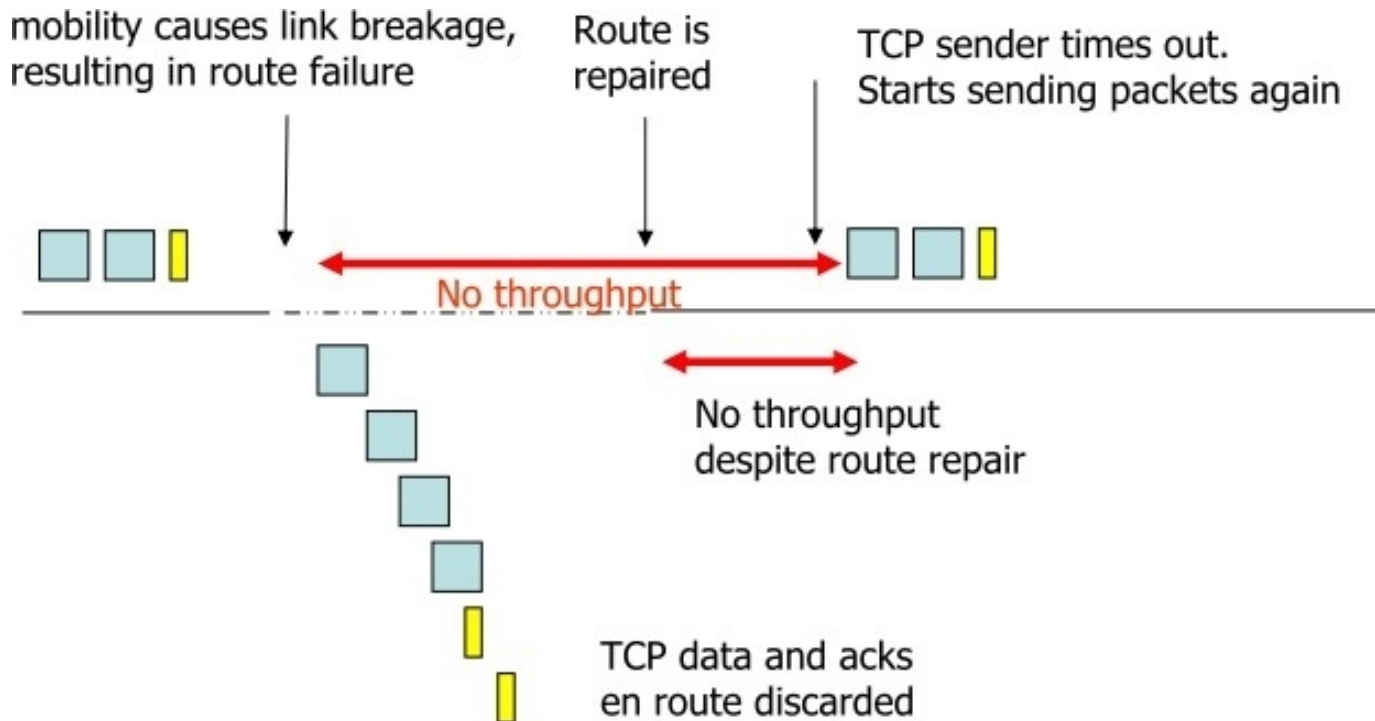


Image source: [Vaidya, Infocom 2004]

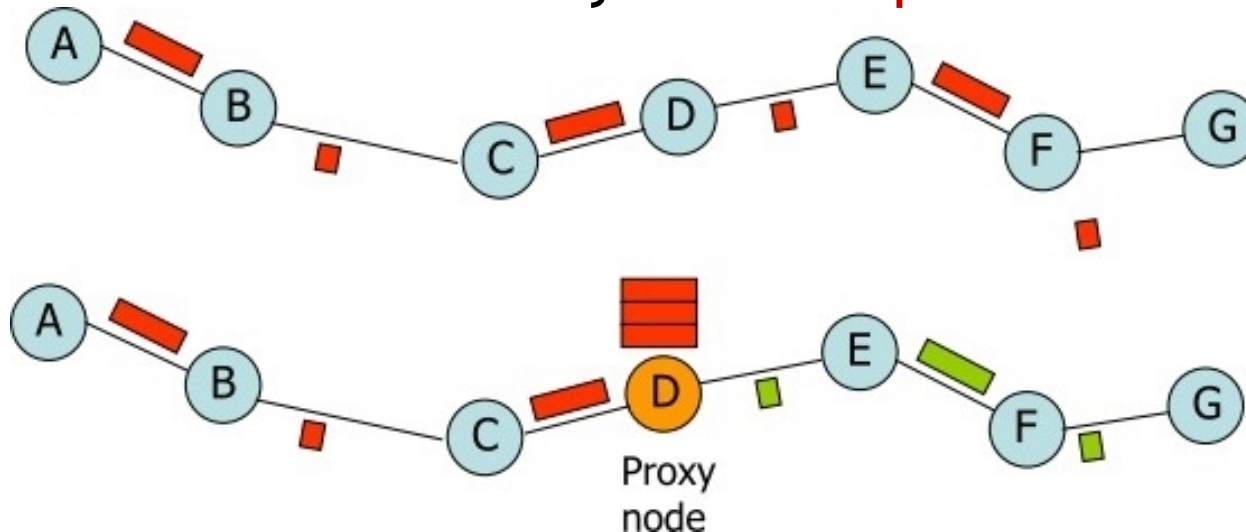
# Routing → Transport Impact

- Route caching interferes with TCP (e.g., in DSR)
  - Multiple routes stored to reduce discovery overhead
  - At network layer, source scans for a live route
    - Older routes may have been broken due to mobility, etc.
    - Successive TCP timeouts, lack of data traffic during scan of the cached routes
  - Instead:
    - Deactivate route caching
    - Explicit link failure notification (TCP-ELFN)
    - Explicit congestion notification or ICMP unreachable messages (ATCP)



# Split TCP

- In mixed wired/wireless:
  - TCP runs only at the end-points and at a proxy at the wired/wireless border
  - Proxy accelerates traffic through wired domain
- In wireless multihop:
  - Proxies can be similarly **used to split into short paths**



# Split TCP Pros/Cons

- Pros:
  - Improves multi-hop TCP opportunity using shorter loops and faster evolution
  - Retransmissions follow shorter paths, saving energy and reducing interference
- Cons:
  - Breaks E2E, so no longer compatible with end-to-end security such as IPSec
  - Increased buffering at proxies, required greater intelligence at intermediate nodes
  - Route changes/breaks require proxy changes

# Misbehavior

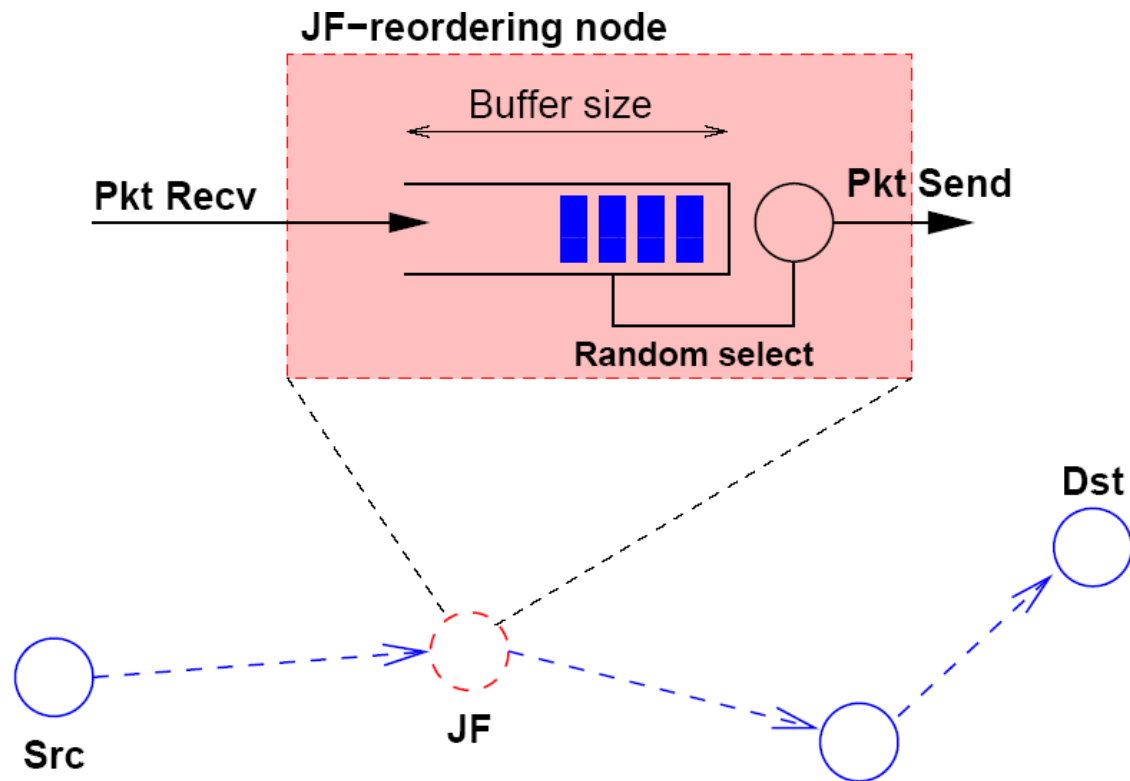
# JellyFish Attacks

[Aad, Hubaux, and Knightly; MobiCom 2004]

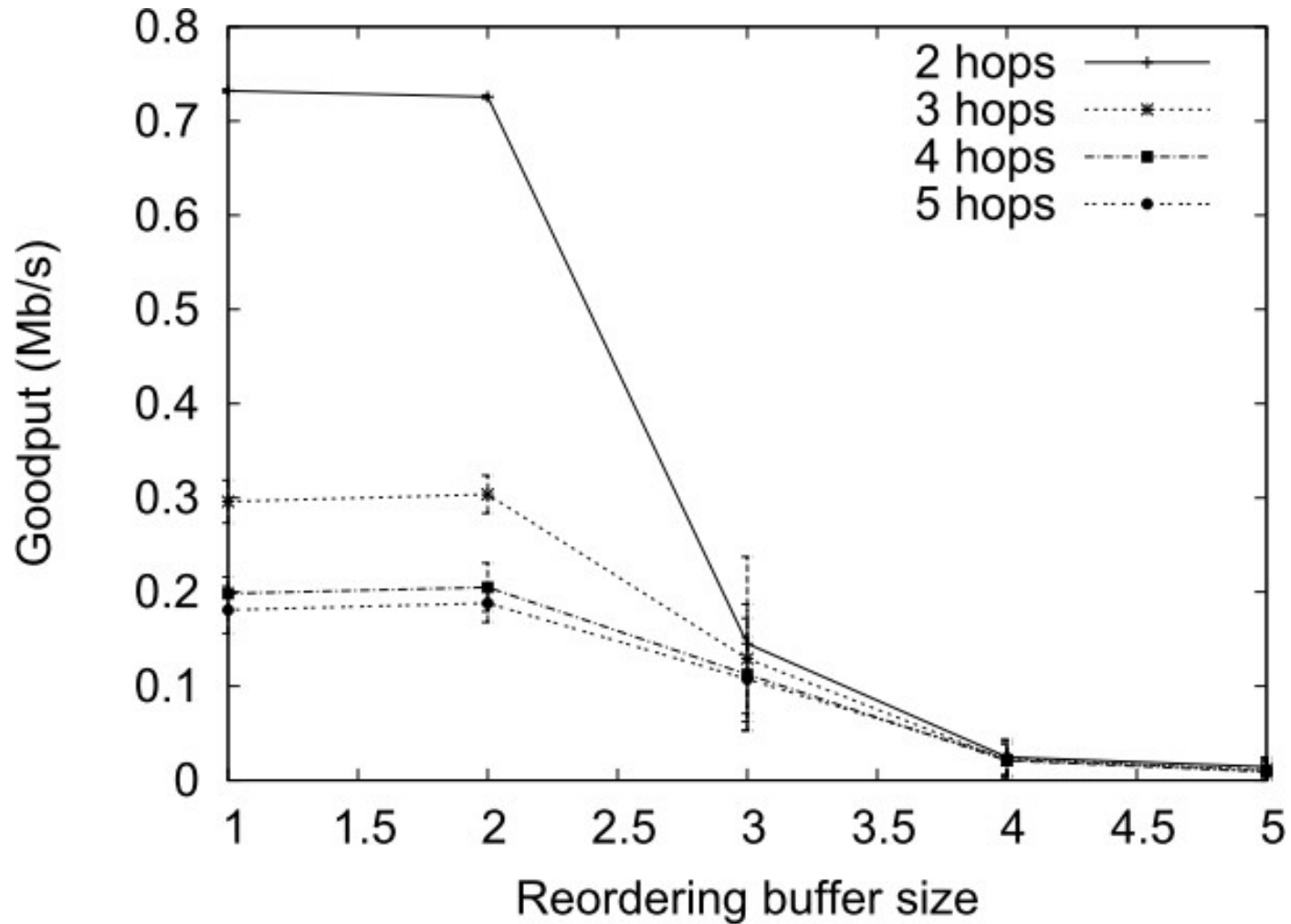
- JellyFish (JF) attacks target congestion control used in many TCP and UDP variants
  - JF attacks comply with all control and data plane protocol requirements except for targeted malicious actions including:
    - Re-ordering packets
    - Periodically dropping packets
    - Increasing delay variance

# JF Re-ordering

- TCP uses cumulative ACKs for efficiency and rely on duplicate ACKs to detect loss or out-of-order reception
  - All TCP variants assume that **packet re-ordering is a relatively rare and short-lived event**
- JF Re-ordering attack
  - Deliver all **packets** but **using a re-ordering queue** instead of a FIFO queue

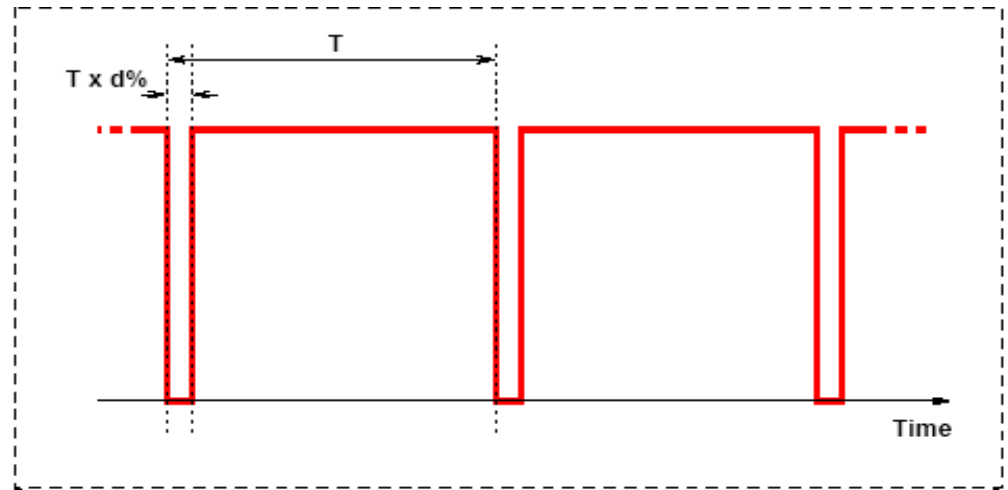


# Impact of JF Re-ordering



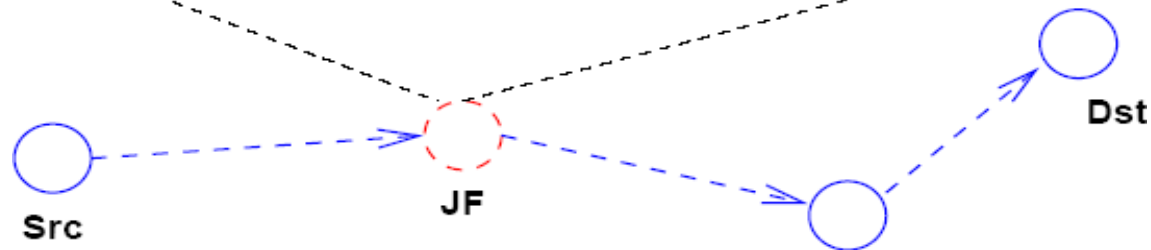
# JF Periodic Dropping

- If packet loss occurs periodically near the retransmission time out scale ( $\sim 1s$  to address severe congestion), then E2E throughput is nearly zero



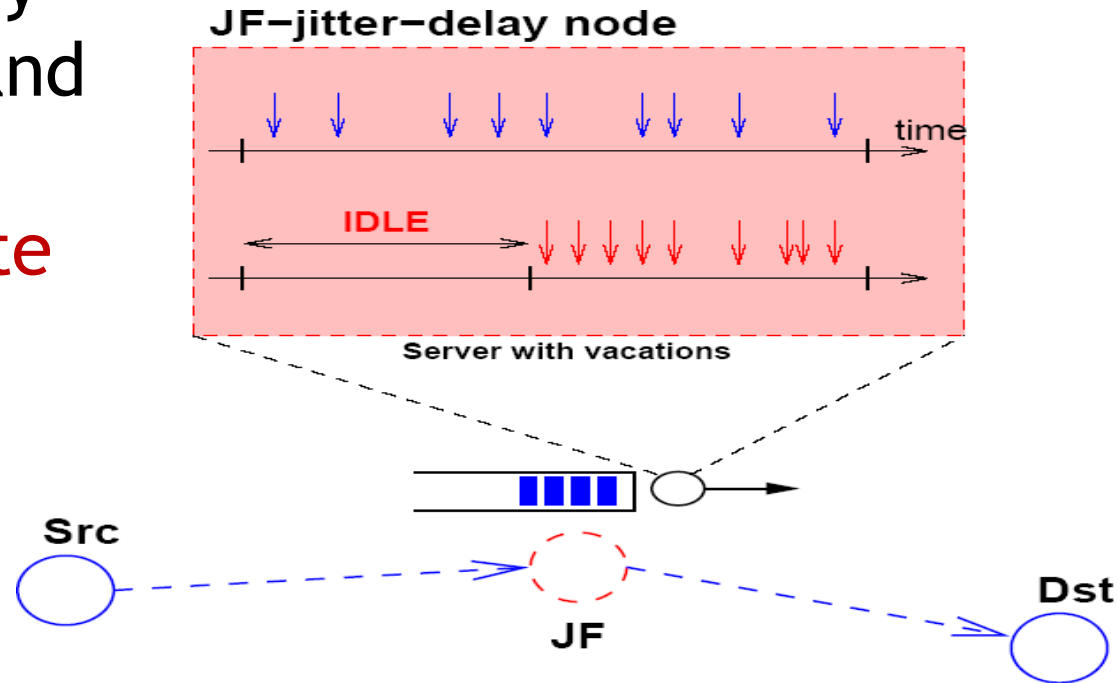
- JF periodic dropping attack

- Drop packets for a very short duration with period near the retransmission time out



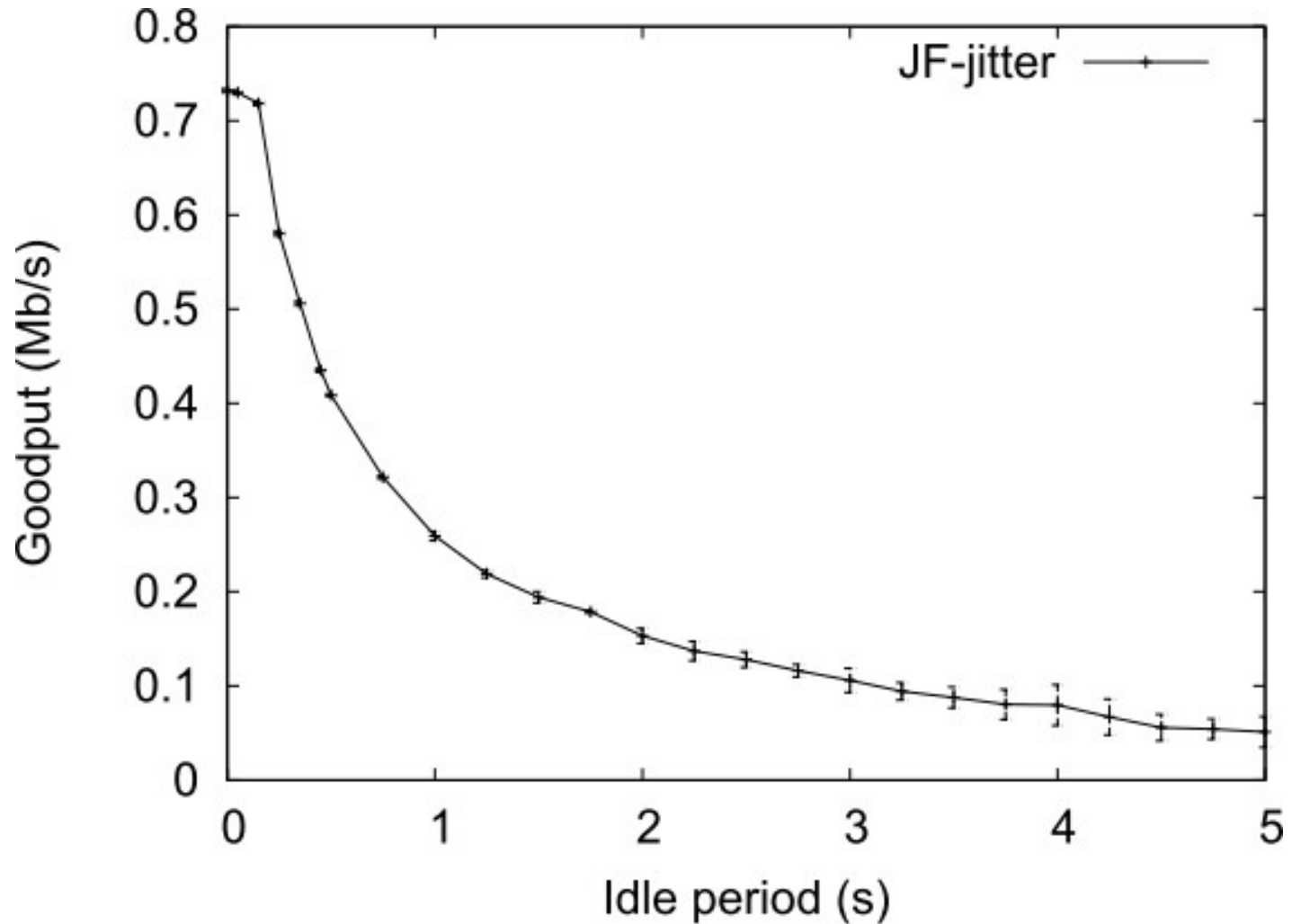
# JF Delay Variance

- Round-trip times vary due to congestion, and **this variance is measured to estimate important protocol parameters**
- JF delay variance attack
  - **Inject random delay in forwarding each packet, maintaining order, but increasing delay variance**





# Impact of JF Delay Variance



# Detection of JF Attacks

- Detection relies on **ability to monitor forwarding behavior**
  - Using passive ACK or “overhearing” (e.g., Watchdog)
  - Lots of analysis and simulation in the paper
- Upon detection, victim can:
  - Change routing path
  - Switch to multi-path routing
  - Create backup routes to use when performance drops

What about transport protocols  
other than TCP and UDP?

# WSN Transport Reliability

[Buttyán and Csik; PerSens 2010]

- Researchers have proposed many alternative transport mechanisms for WSNs
  - **ACK-based approaches**, either on an end-to-end or hop-by-hop basis
- Transport-layer attacker
  - Eavesdrops on communications in the network, forges and injects transport-layer control messages
    1. Attacks against reliability
    2. Energy depletion attacks

# Summary

- Transport-layer misbehavior types and potential defenses
  - Jellyfish attacks and protocol-compliant misbehavior in TCP and reliable UDP settings
    - [Aad et al.; MobiCom 2004]
  - Misbehavior in alternative transport protocols for wireless sensor networks
    - [Buttyan and Csik; PerSens 2010]