Analysis of Attacks and Defense Mechanisms for QoS Signaling Protocols in MANETs

by Charikleia Zouridaki

Charikleia Zouridaki¹, Marek Hejmo¹, Brian L. Mark¹, Roshan K. Thomas², and Kris Gaj¹

¹ECE Dept., George Mason University, U.S.A.
²SPARTA, Inc., USA
Agenda

1. Introduction

2. Vulnerabilities in QoS Signaling for MANETs

3. Analysis of Attacks and Defense Mechanisms for QoS Signaling

4. Conclusion
Background: The SEQUOIA Project:
Security and Quality Of Service In Mobile Ad hoc Networks

- How do we integrate security and QoS requirements into routing protocols for MANETS?
Introduction

• Work on MANET security has focused on (1) key management, (2) secure routing
  • do not address the issues of QoS attacks and DoS

• Cryptographic techniques can/should also be applied to QoS signaling
  • but they can address a subset of the security problems

• For Example: an attacker being part of a “secure” route may
  • comply with a secure routing protocol
  • but attack and exploit the signaling protocol

• Securing QoS signaling is challenging
  • attacks are difficult to distinguish from network congestion or connectivity loss

• Goal: analyze a representative class of attacks targeted at QoS signaling in MANETs and identify the key elements required in a secure QoS signaling scheme
Background - QoS Signaling in MANETs

- 2 types of signaling protocols:
  - reservation-based (INSIGNIA)
  - reservation-less QoS signaling (SWAN)

- When needed, the attacks will be illustrated by applying them to INSIGNIA and SWAN for simplicity

- INSIGNIA basics:
  - control information is exchanged between S-D to reserve, renegotiate, and release resources per flow

- SWAN basics:
  - S probes for available resources along a route
Vulnerabilities in QoS Signaling for MANETs

- Open network topology
  - Overlaps in radio transmission/reception ranges

- Node mobility
  - Address, node identity are independent of a node’s location

- Intermittent connectivity
  - control messages may be lost
  - protocol timing dependencies may be modulated

- Limited node capabilities
  - energy, memory, and CPU cycles
Analysis of Attacks and Defense Mechanisms for QoS Signaling

• Assumption:
  • secure routing protocol is in place!

• Attack analysis follows a 3-component template:
  • Vulnerability:
    – the network state or property that the attacker exploits
  • Attack Step:
    – the method by which the attacker carries out the attack, the position of the attacker in the network, the amount of effort used by the attacker, etc.
  • Effect:
    – the observable effects and side-effects of the attack
Attacks on reservation-based QoS signaling, 1/2

Over-reservation:

- **Attack analysis:**
  - **Vulnerability:** 1. protocol cannot verify usage of reservations, 2. naive refreshment of reservations (e.g., INSIGNIA)
  - **Step:** attacker 1. acts as the source node, 2. requests more bandwidth than it uses, 3. sends one data packet in the specified refresh-time interval to refresh the reservation
  - **Effect:** 1. bandwidth under-utilization, 2. legitimate sessions are denied service

- **Issues specific to MANETs:**
  - 1. the wireless channel provides small capacities, 2. straightforward techniques for rate monitoring is node overwhelming

- **Countermeasure:**
  - data rate monitoring and rate adjustment performed by each node traffic flows through a node are aggregated and managed on an in-hop/out-hop basis (DRQoS)
State Table Starvation:

- **Attack analysis:**
  - **Vulnerability:** 1. node has limited memory and computational power, 2. reservations are made on a per flow basis, 3. protocol cannot verify usage of reservations
  - **Step:** attacker 1. acts as the source of the data packets, 2. requests bandwidth for an illegitimate RT flow
  - **Effect:** 1. state table is exhausted, 2. legitimate sessions are denied service

- **Issues specific to MANETs:**
  - Mobile devices have significant memory constraints

- **Countermeasure:**
  - state table of node to grow as a function of the number of neighbor nodes $\rightarrow N$ neighbors: max number of in-out flows per node = $N(N-1)$ (DRQoS)
General attacks on QoS signaling, 1/5

Over/under reporting of available bandwidth: (example: SWAN)

- **Attack analysis:**
  - **Vulnerability:** 1. bandwidth availability is perceived uniquely by each nodes, 2. link capacities are not fixed, 3. protocol is unable to validate the available bandwidth reported
  - **Step:** attacker 1. acts as an intermediate node, 2. falsely represents the available bandwidth
  - **Effect:** S sends at a rate that does not match the available bandwidth on the path

- **Issues specific to MANETs:** link capacities frequently change

- **Countermeasure:**
  - over-reporting: 1. detected at the application layer by D, 2. isolating the misbehaving node by triggering a new route search, 3. information provided to an IDS to isolate the attacking node
  - Under-reporting: 1. signaling protocol triggers a new route search → extra overhead, 2. IDS logs information on resources reported by nodes on different routes and detects inconsistencies
QoS Degradation: new class of attacks in QoS signaling

- **Attack analysis:**
  - **Vulnerability:** protocol does not verify QoS performance
  - **Step:** attacker 1. acts as an intermediate node, 2. increases the delay or jitter of the data packets to unacceptable levels
  - **Effect:** 1. QoS for a particular service is degraded, 2. real-time session needs to be re-initiated

- **Issues specific to MANETs:**
  - QoS degradation attacks are difficult to distinguish from impairments caused by node mobility or intermittent connectivity

- **Countermeasure:**
  - Conventional DoS mitigation techniques cannot recognize the increase on delay or jitter
  - 1. detected at the application layer by D. 2. trigger a search for a new route, 3. report to an IDS
General attacks on QoS signaling, 3/5

Timing Attack:
(example: SWAN)

- **Attack analysis:**
  - **Vulnerability:** 1. protocol has timing dependencies, 2. compliance to protocol is not checked
  - **Step:** attacker 1. acts as the source or destination node, 2. exploits the timing dependencies
  - **Effect:** attacker gains access to the channel at the expense of legitimate flows

- **Issues specific to MANETs:**
  - intermittent connectivity & dynamic topology cannot guarantee that a message will arrive at the D (on time) → timing attacks might not be recognized

- **Countermeasure:**
  - a QoS signaling scheme that does not present time dependencies & does not employ timers to control the protocol’s behavior (like DRQoS, INSIGNIA)
General attacks on QoS signaling, 4/5

**Flooding:** send traffic above the negotiated rate

- **Attack analysis:**
  - **Vulnerability:** protocol 1. does not verify resource usage, 2. does not identify the source of flooding, 3. does not take measures against flooding
  - **Step:** attacker 1. acts as the source node, 2. floods the network with traffic
  - **Effect:** 1. network is flooded, 2. legitimate sessions are denied service

- **Issues specific to MANETs:**
  - challenging to trace back an attacker in MANET

- **Countermeasure:**
  - aggregate traffic streams policed on an in-hop/out-hop basis → a flooding flow experiences traffic policing by at least one of the intermediate nodes on the path (DRQoS)
General attacks on QoS signaling, 5/5

Replay Attack:

- **Attack analysis:**
  - **Vulnerability:** 1. protocol does not protect the integrity of signaling information, 2. protocol cannot distinguish a replay from an authentic message, 3. open topology
  - **Step:** attacker 1. duplicates/modifies signaling information, 2. forwards modified packet to the next hop
  - **Effect:** 1. resources are wasted by illegitimate packets, 2. legitimate packets are denied service

- **Issues specific to MANETs:**
  - broadcast medium → each node hears the transmission of every node in its radio transmission range

- **Countermeasure:**
  - limited number of replayed packets processed over a time interval
DRQoS: DoS Resistant QoS Signaling Protocol

  - reservations on in-hop/out-hop basis
  - distributed traffic policing
  - distributed rate monitoring and adjustments

- DRQoS addresses the following attacks:
  - Over-reservations
  - State Table Starvation
  - Timing
  - Flooding

- DRQoS does not address the following attacks:
  - Over/under-reporting
  - QoS Degradation
  - Replay
Conclusion

• A complete solution to secure QoS signaling solution for MANETs should incorporate the following elements
  1. intelligent traffic management (DRQoS)
  2. lightweight intrusion detection (distributed trust establishment schemes, Buchegger)
  3. efficient cryptographic primitives (symmetric cryptosystems, ECC PKI, key chains)

• Ongoing work
  • we are further developing the DRQoS scheme
  • investigating computationally lightweight schemes to establish trust measures for MANETs
Thank you!

Questions?