Survivable Routing in Ad Hoc Wireless Networks

Cristina Nita-Rotaru

Joint work with
Baruch Awerbuch, Reza Curtmola, Dave Holmer and Herb Rubens
Johns Hopkins University
Bogdan Carbunar, Ioannis Ioannidis,
Purdue University

IUPUI - 1 April 2005
Wireless Revolution

- **WiFi ad hoc networks**: infrastructure-less, distributed routing, maintenance built within the network, quick and cost-effective deployment.

- **Cellular networks**: 3G cellular networks promise us multimedia contents (already provided in Japan by DoCoMo and in Europe by Vodafone).

- **Mesh Networks**: structured (mesh) wireless networks, providing the ‘last mile’. (cities like NYC and Phily; companies:Tropos, Flarion, Motorola, MeshNetworks, etc.).
Why You Should Care About Security

- **Access control**: Lack of access control can translate into degradation of service (medium is shared)
- **Confidentiality**: medium is open and easy to eavesdrop
- **Relay**: multi-hop networks, nodes rely on un-trusted nodes to transport data
- **Physical security**: wireless devices are more likely to be stolen
- **Challenges**: mobility, energy constraints, vulnerable to jamming of the channel, decentralized environment
Survivability Concepts

Survivable protocols are able to provide correct service in the presence of attacks and failures.

- **Fault-tolerance**: benign failures (network partitions and merges, process crashes).
- **Confidentiality**: protects from eavesdropping.
- **Active attacks**: impersonation, replay attacks.
- **Denial of service**: resource consumption.
- **Internal attacks**: part of the infrastructure is compromised.

Byzantine adversary: an adversary that can do anything.
Focus of This Talk

**Goal:** routing protocols for multi-hop (or hybrid) wireless networks that can provide correct service in the presence of compromised participants, as long as a correct (non-adversarial) path exists between source and destination.

**Challenges:** mobility, decentralized environment, prone to errors, difficult to distinguish between failures and malicious behavior.
Outline

- **Attacks against routing in ad hoc wireless networks**
- **ODSBR**
  - Goals and approach
  - Protocol description
  - Simulations showing attack mitigation
- **JANUS**
  - Goals and approach
  - Protocol description
- **Current and future work**
Routing in Ad Hoc Wireless Networks

- On-demand protocols preferred because of lower overhead
- General mechanism:
  - On-demand: look for a path only when need to route
  - Flood to find a path to the destination, then use the reverse path to inform the source about the path
  - Use duplicate suppression technique, only first flood that reaches a node is processed, next are discarded (all have the same identifier, higher identifiers denote new requests)
  - Shortest path is selected based on a metric: AODV uses a hop count, while DSR uses the shortest recorded path
  - Nodes cache discovered routes
  - Route maintenance mechanisms, nodes report broken links
Example: Dynamic Source Routing (DSR)

Route Discovery

- Source broadcasts route request (RREQ) packet specifying the destination; RREQ carry unique identifiers
- An intermediary node receiving RREQ, verifies if he has seen it before:
  - Yes: discard
  - No: appends its address to a list in the RREQ and rebroadcasts it
- Destination receives RREQ, it sends route reply (RREP) back to source of RREQ with a copy of the accumulated address list from RREQ
- RREP reaches source of RREQ, it caches the new route in its cache
Example: DSR (cont.)

**Route Maintenance**

- If a node on the path does not get an ack after a limited number of local retransmissions it generates a route error (RERR) message back to source identifying the broken link.
- Source then removes path containing broken link from cache.
- Source will use an alternate route to destination (if one exists in cache) or it initiates a new route discovery.
Fabrication and Modification Attacks

- Change the path on the request packet and forward it
- Generate false request messages to burden the network
- Spoof IP address and send request
- Send false route replies, modify replies, false topology
- Send higher sequence numbers
- Result: Nodes can add to a path and make it less probable that the “shortest path” is through them, or can shorten paths to make it more likely they are on paths. Use this to either avoid forwarding traffic, or for traffic analysis.

**Attack is possible because of lack of hop-by-hop integrity and authentication of the packets.**
Fabrication and Modification Attacks (cont.)

- Generate false route error messages
- Drop route error messages
- Spoof IP address and send error message for a valid route
- Result: Attacker can continually tear down routes with false error messages, or by not reporting the error, packets will be lost.

*Attack is possible because of lack of integrity and authentication of the packets.*
The wormhole turns many adversarial hops into one virtual hop creating shortcuts in the network.

Attacker (or colluding attackers) records a packet at one location in the network, tunnels the packet to another location, and replays it there.

PACKETS LOOK LEGITIMATE, authentication and freshness mechanisms not enough.

Result: Allows an adversary to control path selection.

Attack is possible because of lack of a mechanism that controls that packets traveled on shortcuts.
Flood Rushing Attacks

- Attacker disseminates request quickly throughout the network suppressing any later legitimate request
  - By avoiding the delays that are part of the design of both routing and MAC (802.11b) protocols
  - By sending at a higher wireless transmission level
  - By using a wormhole to rush the packets ahead of the normal flow
- Result: no path is established, or an attacker gets selected on many paths

**Attack is possible because of flood request suppressing technique and attacker can rush packets through the network.**
Misbehaving Nodes

- Ad hoc networks maximize total network throughput by using all available nodes for routing and forwarding.
- A node may misbehave by agreeing to forward the packet and then failing to do so because it is selfish, malicious (black holes) or fails (errors).
- Result: throughput drops

*Challenge:* distinguish between the above 3 types of behavior.
Summary of Attacks on Wireless Networks

- Types of Attacks
  - Eavesdropping
  - Impersonation
  - Fabrication
  - Modification
  - Replay
  - Flood rushing
  - Denial of service
  - Blackhole
  - Wormhole

- Types of Adversaries
  - Individual /Colluding
  - Outsiders/ Insiders (Byzantine)

- Place of attack
  - Routing mechanisms
  - Data forwarding
Related Work

- Wormhole: Hu, Perrig, Johnson - 2003a
- Flood rushing: Hu, Perrig, Johnson - 2003b

NO PROTOCOL ADDRESSING ALL ATTACKS!
Outline

- Attacks against routing in ad hoc wireless networks
  - ODSBR
    - Goals and approach
    - Protocol description
    - Simulations showing attack mitigation
  - JANUS
    - Goals and approach
    - Protocol description
  - Current and future work
ODSBR: Goals

- Assuming that there exists a correct path between source and destination, ODSBR finds it and delivers data between source and destination in spite of compromised and colluding Byzantine nodes.
- Limit the amount of damage an attacker can create to the network
- Do not partition the network

ODSBR Mechanisms

- Hop-by-hop protection, intermediate nodes are authenticated but not trusted
- Instead of preventing wormholes formation, detect them if they cause problems
- Use a link reliability metric in which suspect links are avoided regardless of actual reason for detection
  - Malicious behavior
  - Adverse network behavior (bursting traffic)
  - Shelfish or failures
ODSBR Overview

Route Discovery with Fault Avoidance

Discovered Path

Byzantine Fault Detection

Weight List

Link Weight Management

Faulty Links

ODSBR Description
Route Discovery

- Bi-directional flood
- Distance vector protocol, based on single source Bellman-Ford
- Uses weight list contained in request
- Only lower cost updates are broadcast
- Path is accumulated on response packet
- Each hop appends an identifier and signature
- Path is verified at intermediate nodes to prevent flood blocking attack
Fault Identification

- **Definition of fault**
  - Violation of a fixed loss threshold
  - Excessive delay

- **Probe list**
  - Masked in the data traffic
  - Cryptographic mechanisms are used to ensure that no node can see who else is asked to ack (prevents blacklisting)

- **Ack**
  - Authentication via HMAC and onion encrypted
  - Combined at each probe point or can be piggy-backed on transport level acknowledgement

- **Error messages**
  - A node can not be prevented from reporting a link he is one of the nodes, as broken, but we can prevent errors reported on links he is not part of.
Fault Detection Strategy

- Use authenticated acknowledgements from nodes on the path (requires source routing)
- Probing technique: ask every node to send acknowledgements
Adaptive Probing

Source

Destination

Success

Fault 1

Fault 2

Fault 3

Fault 4

Trusted End Point

Successful Probe

Successful Interval

Intermediate Router

Failed Probe

Failed Interval

Fault Location

Unknown Interval

ODSBR Description
Link Weight Management

- Identified faulty links have their weight doubled
- Links are reset after a period of undisturbed operation
- Bounded total number of packets lost while finding a “good” path

\[ q^p q^+ < b k \log_2 n \]
Simulations Setup

- Parameters: Loss threshold rate: 10%, Link timeout: 250 ms, Sliding window size: 100 packets.
- 802.11b: bandwidth of 2 Mbps and nominal range 250 m.
- 50 nodes _ 0-10 adversaries placed within a 1000 by 1000 m² area
- Traffic load: 10 CBR flows, an aggregate load of 0.1 Mbps each flow send 256 byte packets at approximately 4.9 packets/second.
- Simulation time was 300 seconds, results were averaged over 30 random seeds.
- Nodes select a speed between 10% and 90% of the given "max" and 300 virtual seconds of mobility are generated before the start of the simulation.

Blackhole and Flood Rush

Flood rushing helps the attacker to get selected on more paths, thus he can create more damage.
Wormhole Central Configuration

ODSBR not affected by flood rushing, while one wormhole centrally placed creates significant damage.
Wormhole Overlay: Complete Coverage

Simulations

Delivery ratio of AODV drops to 20%. 5 Adversaries completely control a network of 50 nodes.
ODSBR: Summary

- Most important factors for an effective attack: flood rushing and strategic positioning of adversaries.
- Two colluding adversaries forming a central wormhole combined with flood rushing can mount an attack that has the highest relative strength, it reduced AODV's delivery ratio to 51%.
- ODSBR was able to mitigate a wide range of Byzantine attacks; not significantly affected by flood rushing. Its performance only decreased when it needed to detect and avoid a large number of adversarial links.
Outline

- Attacks against routing in ad hoc wireless networks
- ODSBR
  - Goals and approach
  - Protocol description
  - Simulations showing attack mitigation
- JANUS
  - Goals and approach
  - Protocol description
- Current and future work
Cellular Networks: 3rd generation

- GSM (Europe), IS-136 (USDC) and PDC (Japan) evolved into UMTS/W-CDMA
- IS-95(cdmaOne) evolved into cdma2000
- W-CDMA promises 2.0Mbps download rates
- cdma 2000 1xEV-DO, provided by Qualcomm promises 2.4Mbps instantaneous High Data Rate for Data Only transfers
Distance vs. Bandwidth

- Quality of service degrades quickly with the distance from the cellular base station
- UCAN solution [Luo et al ‘03]: use dual interface cellular/802.11b network cards; remote devices can find an ad-hoc path to devices with better cellular access;
- Problems to solve …
  - Security concerns raised because of the new communication model
  - Improving the efficiency in terms of communication overhead imposed and throughput achieved
Janus: Goals

- Provide a protocol that provides secure routing, path reservation and data forwarding, in an environment where every node trusts the base station, assuming that there is a correct path between the client node and base station.

Security Issues: the Usual Suspects

- Impersonation: obtain free of charge services or frame other hosts
- Rate inflation: advertise larger cellular or ad-hoc rates
- Tunneling: non-adjacent hosts can advertise an excellent rate between them; done using a route of mobile hosts or even the BS.
- Denial of service: generate arbitrary traffic without paying for it
- Black hole: malicious relayers can selectively drop packets instead of forwarding them
- **Caveat:** hosts always have their cellular link; thus, malicious behavior cannot prevent them from getting the service via the cellular link from BS
- **However…** rate inflation and tunneling attacks can lure hosts into choosing worse paths, effectively reducing their throughput and undermining their faith in the system …
Systems and Security Assumptions

- Each host is in the transmission range of the cellular base station
- BS has an account for each host
- BS is trusted by all the hosts and can establish secure channels with each host
- Hosts can be authenticated by BS
- Hosts have GPS receivers providing verifiable positions
Janus Overview

- **Secure routing path maintenance**: maintain a routing tree of the network
- **Secure path reservation**: reserve resources for a download
- **Secure data forwarding**: the actual download procedure
Path Maintenance

- Simple approach: greedily seek the device with the highest downlink rate
- Pitfalls: overlooks
  - the limited bandwidth of ad-hoc links
  - the effects of congestion
- Our approach: lazily maintain a maximum spanning tree of the residual network
  - The MST guarantees the path with the maximum minimum link throughput
Topology Trees

- JANUS maintains
  - locally: *routing tree* rooted at BS
  - at BS: *topology tree* [Frederickson ’97]
  - 4 operations: *cut, link, mincost, update*
- Topology tree ensures $O(\log n)$ complexity per operation

Routing path maintenance
Path reservation
Data forwarding

Routing tree + clustering illustration
Topology tree
Tree Operations

- **Cut(v)**: remove the edge between host v and its parent
  - host v contacts BS on its secure cellular channel
- **Link(u, v, w)**: merge the routing trees rooted at u and v by making v the parent of u, with w the throughput of the connecting link
  - hosts u and v locally evaluate w; contact BS with w and their verifiable positions
  - BS verifies the accuracy of w before updating the topology tree
  - prevents rate inflation and tunneling attacks
- **Mincost(v)**: reveal the throughput of the weakest link on the path between v and BS
  - any host can obtain the value from BS
Secure Path Reservation

- When a host A needs to download information from BS
  - traverse the routing tree following the parent links
  - intermediate nodes can refuse or confirm their participation and commit to the available resources

- Update(v, w): add value w to the throughput of all links between v and BS
  - BS supervises the operation by monitoring the existing flows
Secure Data Forwarding

- After BS receives a valid reservation message from host C requested by A, it initiates the data forwarding phase
  - retrieve the information requested
  - encrypt it with the key shared with A
  - fragment the result into packets
  - forward packets to C
- A acknowledges received packets to BS
- Non-ack packets trigger a binary search of the black hole as in ODSBR
- Advantage: all control traffic (probe request and acks are sent on the cellular link).
Summary

- Securing a hybrid network having a cellular component is an easier task because
  - There exist a centralized entity (BS) in the system
  - Direct cellular links prevent blacklisting
- There are still problems to be solved: how to obtain verifiable position when GPS can also be cheated
- Better solution in dealing with interference.
Current and Future Work

- Provide a protocol aware of interference from other flows.
- Extend the model to other hybrid networks.
- Consider the case of multiple base stations controlled by a single authority or multiple, potentially distrustful authorities.
- Apply similar techniques to mesh networks.
- Investigate attacks against MAC protocols.
Contact Information

- Email: crisn@cs.purdue.edu
- Google: Nita-Rotaru
- URL:
  http://www.cerias.purdue.edu/homes/crisn/lab/swan.html

THANK YOU!