Hacking MANET

Building and Breaking Wireless Peering Networks

Riley “Caezar” Eller
Why or Why Not MANET?

• Ideals
  – Allows seamless roaming
  – Works when infrastructure breaks
  – Routing does not require administration
  – Functional in hostile environments
  – Farther from the Shannon curve due to lower typical transmission distance

• Problems
  – Network scalability
  – Effective, voluntary security
Mobile Networking

• People move a lot
• Fast dynamic routing is a hard problem
• Infrastructure solutions are much easier
• Hybrid infrastructure (or “fixed mesh”) reduces the problem somewhat
• People want a real solution
Here Comes the Science

- Major types of network routing protocols
  - Link State
    - Dyikstra SPF algorithm
    - Example: OSPF
  - Distance-Vector
    - Bellman-Ford algorithm
    - Example: RIP
  - Policy Based
    - Policies override core DV or LS style routing algorithms
    - Example: BGP
Distance-Vector Routing

• Values
  – Each device has a unique address
  – Applications don’t distinguish transports
  – Robust during partial failure
  – Perceived to be much more natural by users
  – Allows for a high mobility index

• Challenges
  – High processing complexity
  – High message complexity
Link State Routing

• Values
  – Low processing and message complexity
  – Comparatively inexpensive

• Challenges
  – Each interface has a unique address
  – Applications may require transport specific information, such as locally bound IP address
  – Exceptionally unnatural to users
  – Demands a low mobility index
Godzilla Versus Dyjkstra

- Places where LSR (or equivalents) wins
  - The Internet (except as noted below)
- Places where DVR (or equivalents) wins
  - Mesh networks
  - Interior gateway routing
  - Border gateway routing
  - Games and AI
Infrastructure-Mode Wi-Fi

- **Immobile**
  - Wired equivalency tether
  - Must sacrifice bandwidth exponentially to increase radius linearly
- **Inefficient**
  - Peer to peer messages eat double bandwidth
  - Close security model requires user intervention
Fixed Mesh Wi-Fi

• Marginal improvement at best
  – Client devices still tethered
  – Same scalability problems among access points
  – Reliable fail-over only by sacrificing footprint
  – Does nothing to improve disaster scenario
  – Worse spectrum allocation

• Lagging standard not due until 2008
What We Really Want

• Peer to peer network
  – Excellent security
  – VOIP and 3GPP reliable delivery
  – Automatic discovery
  – Maximum mobility
  – User defined network policy
Understanding the Link Layer

- Understanding mesh links
  - Nodes beacon to provide carrier sense
  - Discover peers automatically
  - Infer link quality from beacon packet reception
  - Acknowledge high quality beacons
  - Translate link quality into link metric, e.g.:
    - For 802.11b, 99% beacon reception implies about 1200 millisecond expected transmission delay
    - 40% reception implies nearly infinite delay
Attacking the Link Layer

- **Eavesdropping**
  - Discover participants and topology
  - Retrieve public keys (identity tracking)
  - Content interception
- **Sybil Attack**
  - Greeting flood
  - Storage or processing denial of service
Attacking the Link Layer

- Greeting and acknowledgement replay
  - Causes link quality overestimate
  - Causes degenerate routing
  - Increases processing and storage requirements
- Wormhole attack
  - Previous work here by S. Swami and others
  - Will discuss in more detail as a routing layer attack
Attacking the Link Layer

• Unauthorized access
  – Bandwidth reduction
  – Perimeter intrusion
• Selective jamming
  – Freeze the Wi-Fi MAC layer
  – Underestimate link quality
  – Isolate and conquer
Securing the Link Layer

- Link Cryptography
  - DH/DSA key exchange
    - Gives clear cryptographic session definition
    - Prone to computational denial of service attacks
  - Work tokens
    - Defend against DOS
    - Leverages desire to join against computation requirements
Securing the Link Layer

• Link Cryptography (continued)
  – Signed broadcasts
    • Exceptional computational cost
    • Prevents wormholes and other forgery attacks
  – Certified identity
    • Translates node identity into comprehensible string
    • Allows user control of policy
    • Impedes unauthorized access
Securing the Link Layer

• Other Techniques
  – Jittered timers
    • Greatly reduces risk of sniping
    • Makes selective jamming very difficult
  – Transient MAC address
    • Avoid manufacturer profiling
    • Cycle periodically to throw off listeners
Avenues for Future Research

• Acknowledgement of hidden nodes
  – Destroy two-hop topology graph
• Ubiquitous acknowledgement
  – Desynchronize link quality estimation
  – Ideal denial of service to perfect links
  – Like a rushing attack, but “from the future” rather than just “faster than allowed”
Understanding the Routing Layer

- Routing is a geometric problem
  - Link quality is driven by signal to noise ratio
  - Signal decreases with the square of distance
- Example
  - $1^2 + 2^2 < 3^2$; thus
  - $AB + BC < AC$; thus
  - A should route through B to reach C
Understanding the Routing Layer

• Understanding mesh routes
  – Advertisement based, e.g.:
    • Node R hears about node O through node P
    • “Receiver hears about Origin through nearby Peer”
    • Shorthand [R: P->O]
  – Requires temporal quality metric, e.g.:
    • Node R expects a message through P to take 3500 milliseconds
    • Shorthand [R: P = 3500]
Understanding the Routing Layer

• Understanding mesh routes (continued)
  – Metric sums over multiple hops, e.g.:
    • [P: O = 3500]
    • [R: O = 3000]
    • [R: P->O = 3500]
    • R->O = 6500
  – Algorithms need help to avoid routing loops
    • Must never accept older or slower information
    • Must track edition numbers to deal with asynchronicity
Attacking the Routing Layer

- Refusal to participate
  - Black hole
    - Drop all data packets
    - Very easy to detect
  - Gray hole
    - Drop some data packets
    - Discoverability proportional to packet drop ratio
Attacking the Routing Layer

• Underestimating distance
  – Wormhole
    • Requires sideband packet forwarding
    • Absorbs all traffic within $(H-1)/2$ hops radius
  – Invariant violation
    • Causes routing loops which may become packet storms

• Rushing attacks
  – Exploits “First past the post” duplicate removal algorithm
  – Example: DNS response spoofing
Attacking the Routing Layer

• Invisible “Million Man March”
  – Sybil attack on steroids
  – Flattens scaling topology
  – Destroys local routing efficiency
Defending the Routing Layer

• Trust-based link selection
  – Assume minimal trust of each peer initially
  – Increase trust slowly, decrease rapidly
  – Apply trust multiplier to advertised link cost
  – Contains and localizes damage by harming reputation of naïve intermediaries
Defending the Routing Layer

• Signed control messages
  – Computationally expensive
  – Eliminates rushing and wormhole attacks

• End-to-end validity probe
  – Augment trust metrics with cryptographically secure data or control message
  – Makes Sybil attacks expensive since identities are periodically required to respond
Conclusions

• With MANET we can have…
  – Discovery
  – Identity
  – Quality
  – Efficiency

• But first we need…
  – Scalable routing algorithm
  – Hardware cryptography
  – Fixes for 802.11 Ad Hoc
Going Forward

• What you can do to hurry the future
  – Seek out and play with emerging protocols
  – Develop P2P phone applications
  – Demand hardware crypto on small devices
  – Use Thin-MAC wireless cards
  – Hack It!