ANODR: ANonymous On-Demand Routing with Untraceable Routes for Mobile Ad Hoc Networks

MobiHOC 2003
June 3, 2003

Jiejun Kong, Xiaoyan Hong
Wireless-Adaptive-Mobility Laboratory
Department of Computer Science
University of California, Los Angeles

Passive Routing Attacks in MANET

Location Privacy Attack:
Correlate nodes' ids and their locations

Motion Inference Attack:
Visualize nodes' motion patterns

Route Tracing Attack:
Visualize (multi-hop) ad hoc routes
Passive Routing Attacks in MANET

- **Location privacy attack**
  - Correlate a mobile node with its locations (at the granularity of adversary’s adjustable radio receiving range)
  - Counting/analyzing mobile nodes in a cell
- **Route tracing attack**
  - Visualizing ad hoc routes
- **Motion inference attack**
  - Visualizing motion patterns of mobile nodes
  - Deducing motion pattern of a set of nodes
- **Other traffic analysis**
  - Analyzing packet flow metrics (as in Internet traffic analysis)
- **Orthogonal** to routing disruption attacks

Adversary in Mobile Ad Hoc Networks

- **External adversary**: wireless link intruder
  - Eavesdropper
  - Traffic analyst (not necessary to break cryptosystem)
  - *Unbounded* interception: adversary can sniff anywhere anytime
- **Internal adversary**: mobile node intruder
  - Capture, compromise, tamper
  - **Passive internal adversary** is hard to detect due to lack of exhibition of malicious behavior
  - **Bounded**: otherwise secure networking is impossible
Problems of Ad Hoc Routing

✓ Must rely on neighbors in data forwarding
  – Neighbors need to know routing info
  – “I can forward your packets”: All existing ad hoc routing protocols reveal nodes’ identity to its neighbors — abundant chances for passive attackers to obtain static info

✓ [MobiHOC’01, BasagniHBR] Encrypted routing information can be decrypted by other internal nodes
  – Traceable by traffic analysts (without compromising cryptographically protected information)
  – Allows internal adversary, no location privacy support

Motivations for New Secure Routing

✓ Resistance against location privacy, route tracing, motion inference attacks
  – Using established security methodologies

✓ Efficiency
  – Comparable to existing ad hoc routing schemes

✓ Low probability of detection, interception, and exploitation (LPD/LPI/LPE)
  – Focus on data forwarding, not on physical layer radio signal processing
Related Work

- Other on-demand routing
  - DSR, AODV
- Other anonymity research for wired network
  - Onion routing, Crowds, Hordes
- Other MANET security protocols with orthogonal goals
  - For routing integrity: SEAD, Ariadne, ARAN, etc.
  - For network access control: URSA, etc.
- Either do not address anonymity & untraceability concerns, or not fit in MANET

Design Challenges

- Passive traffic analysis
  - Side channels: time correlation, content correlation
- Passive internal adversary
  - Simple encryption does not solve the problem
- Intrusion Tolerance
  - No single point of compromise or failure
  - Fully distributed design, no centralized control in MANET
- Avoid expensive processing overheads
  - Our measurement & simulation show expensive processing overheads cause non-trivial routing performance degradation
Goal and Design

✓ Efficient routing while anonymous & untraceable to all thy (legitimate & adversarial) neighbors: Mission impossible?

✓ Clues: MANET on-demand routing likely has two broadcast mechanisms
  – Global route discovery (aka. RREQ flooding)
  – Per-hop wireless local radio broadcast

✓ Our design
  – On demand routing
  – Broadcast with anonymous trapdoor assignment
Framework of Anonymous Route Discovery (between src and dest)

✓ Similar to existing on demand routing schemes
  – Route-REQquest
    \(\text{\{RREQ,seqnum, to\_be\_opened\_by\_dest anonymous\_trapdoor\}}\)
  – Route-REPly
    \(\text{\{RREP, presented\_by\_dest anonymous\_proof\}}\)
✓ A global trapdoor can only be opened by dest
  – Not required to know where dest is
  – dest can present an anonymous proof of door opening
✓ Need more design to address per-hop

Per-hop Local Wireless Broadcast with Anonymous Trapdoor Assignment

✓ Trapdoored messages are delivered to specific node(s)
  – But not other nodes in the same receiving group
ANODR Route Discovery
(using TBO - Trapdoor Boomerang Onion)

\[ \text{ANODR: destination } E \text{ receives}\]
\[ \langle \langle \langle \langle \text{RREQ, seqnum, open_by}_E, \text{onion} \rangle \rangle \rangle \rangle \]

\[ \text{where}\]
\[ \text{onion} = K_D(n_s, K_C(n_s, K_B(n_s, K_A(n_s, \text{hello})))) \]

\[ \langle \text{RREP, proof_from}_E, \text{onion, Nym}_X \rangle \]

\[ \text{Nym}_X \text{ is selected by } X \text{ and shared on the hop} \]

Make On demand Routes Untraceable

✓ **ANODR-TBO** is robust against node intrusion
  - Fully anonymous: no node identity revealed
  - Fully distributed control: avoid single point of compromise
  - Multiple paths feasible: avoid single point of failure

✓ So far anonymous only, and symmetric key only
  - More complexity in realizing untraceability to hide side channels & resist traffic analysis

✓ Protect RREP flow
  - Need an asymmetric secret channel
  - Modified RREQ: Embed a temporary asymmetric key \( \text{ecpk}_1 \)
    \[ \langle \text{RREQ, ecpk}_1, \text{seqnum, open_by}_E, \text{onion} \rangle \]
  - Modified RREP: Exchange a secret seed \( \text{Nym} K_{\text{seed}} \)
    \[ \langle \text{RREP, ecpk}_1(K_{\text{seed}}), K_{\text{seed}}(\text{proof_from}_E, \text{onion}) \rangle \]
Make Routes Untraceable (cont’d)

✓ Protect reused route pseudonyms
  – Using $K_{seed}$ to do self-synchronized route pseudonym update
  – So far all pseudonyms/aliases are one-time aliases!

✓ Playout “Mixing”
  – Resist traffic analysis:
    Time correlation
    Content correlation
  – Buffer, Re-order, Batch send, Insert dummy/decoy packets

QualNet® Simulation

✓ Metrics
  – Data delivery ratio, end-to-end latency, normalized overhead, playout “mixing” performance

✓ Impact of
  – Processing overhead (no routing optimization on ANODRs)
    1) AODV with routing optimization and no cryptographic overhead
    2) Anonymous-only ANODR-TBO: symmetric key processing only
    3) Anonymous+Untraceable ANODR-TBO:
      2) limited asymmetric key processing
    4) ANODR-PO, a naive MIX-Net ported from wired networks, asymmetric key processing in anonymous route discovery
  – Communication overhead (≈ 400bit onion, etc.)
  – Mobility
  – Playout “mixing” buffer size $r_x$ & window size $t_x$
Evaluation: Delivery Ratio & Latency (vs. mobility)

- Acceptable delivery ratio degradation for both “anonymous-only” (≈3%) and “anonymous + untraceable” (≈12%) schemes.
- If without untraceability support (which uses asymmetric key cryptosystems), ANODR-TBO’s performance is similar to AODV.
  - Asymmetric key processings cause performance degradation.

Evaluation: Control Packet Overhead (vs. mobility)

- Control packet overhead largely due to onion size.
  - Elliptic curves cryptosystems feature comparable storage (but not latency) overhead with symmetric key cryptosystems.
Evaluation: Playout “Mixing” Performance (vs. $r_x$)

- Playout buffer size $r_x$ and playout time window size $t_x$ are critical parameters
  - In some cases, dummy/data ratio is predictable
- May consume resources like battery power, but does not significantly affect data delivery ratio

Conclusions and Future Work

- Anonymous on demand routing is feasible and efficient in MANET
  - Comparable performance to existing on-demand protocol
  - Intrusion tolerant, esp. against passive adversaries
- Adding untraceable route support is feasible with some efficiency degradation
  - Limited asymmetric key processing
  - Tradeoffs in playout “mixing”
- Future improvements
  - Adaptive “mixing” for better performance
  - Integration with routing integrity countermeasures
  - Multi-path routes to address mobility and disruption