Fundamental Understanding and Theory of Network Systems

Resiliency, Performance, and Usability

Jie Wu
Center for Networked Computing
Temple University
Intractability

- Source and destination location privacy (Panda-hunter game)

- Phantom/Circular Ring Routing
Probabilistic/Controlled Random Routing

Probabilistic Random Routing (PRRP)
- More spread out packets
- Higher hop count and delay

Controlled Random Routing (CRP)
- Less spread in the middle
- Lower hop count and delay

NS3 Simulation
Adversary Model

• Kerckhoffs’s principle: system is public knowledge

• It is unclear how smart an adversary can be

• Traffic analysis challenge: algorithm + big data
  - An adversary can use a sophisticated ML method
  - An adversary can use compressive traffic analysis *(CCS 2017)*

Perform traffic analysis on compressed features instead of raw data
Adaptive Strategic Learning

- Repeated prisoner’s dilemma
  - Cooperate (C) or Defecting (D)
  - Payoff metrics between 1 and 2

\[
\begin{pmatrix}
  C_1 & D_1 \\
  3,3 & 5.0 \\
  0.5 & 1.1
\end{pmatrix}
\]

- Genetic algorithm: mutation and crossover
  - 148 bits with 16 recent states: chromosomes

- From Moore machine to timed automata
  - Adversary’s learning through timing analysis
  - Fitness levels with imperfect information
Adaptive Changes in Structure Hierarchy

• Hierarchical military command chains
• Network hierarchy
  - SDN controllers: load balance and fault tolerance
Self-Organized Systems

Theory community

• Dijkstra’s self-stabilizing system (Dijkstra, 1974)
  - An illegitimate state (caused by some perturbations) can be changed back to a legitimate state in a finite number of steps

• How can we handle the long convergence time that usually occurs in dynamic labeling in a distributed solution? (ICDCS 2017)

Self-Organizing Solutions

Local decision

• P2P and simple interaction (mostly local and without sequential propagation)

Global functionality

• Adaptive, robust, and scalable

Principle

• P₁: Local interactions with global properties (scalability)
• P₂: Minimization of maintained state (usability)
• P₃: Adaptive to changes (self-healing)
• P₄: Implicit coordination (efficiency)

Agility
Broadcasting

Local decision:
backbone nodes
based on node priority
(ID, degree, energy)

Global properties:
Connectivity
Coverage
Self-Healing

• How can we deal with the complexity of building a structure along with a change of topology? (ICDCS 2017)

• Switched-on/off nodes
  - Status changes in 1-hop/2-hop neighbors only

• Seamless integration in a dynamic network
  - Iterative application of a local solution
Resiliency

• Exploiting redundancy: \(K\)-connected & \(K\)-dominated
  - Non-backbone node: if any pair of its neighbors are connected by a path of higher priority nodes
  - Non-backbone node: \(K\) node-disjointed paths for any neighbor pairs

- Moving target defense: IP mutation
Extensions

- Backbone marking works well in **small-world** networks

- In addition to geometric graphs

<table>
<thead>
<tr>
<th>$P$</th>
<th>$CC$</th>
<th>$l$</th>
<th>Backbone</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01</td>
<td>0.96</td>
<td>0.82</td>
<td>1.05</td>
</tr>
<tr>
<td>0.02</td>
<td>0.95</td>
<td>0.75</td>
<td>1.08</td>
</tr>
<tr>
<td>0.03</td>
<td>0.91</td>
<td>0.7</td>
<td>1.1</td>
</tr>
</tbody>
</table>

- $P$:  percentage rewiring
- $l$:  average path length
- $CC$: clustering coefficient
Performance-Security Tradeoff

Dependability includes security
- Mean time between security incidents (MTBSI)
- Mean time to incident discovery (MTTID)
- Mean time to incident recovery (MTTIR)

Performability: work completed before the next security breach

Degradation
- $B_1$: Level 1 breach, 1,000 hrs
- $B_2$: Level 4 breach, 5 hrs

Human factor in discovery and recovery
Conclusions

• Importance of intractability
  - Capability of an adversary

• Importance of self-organized design
  - Basic principles and challenges

• Future
  - A better (graph) model for dynamic networks
    • Intersection graphs and time-evolving graphs
  - Science of security (S & P 2017)
    • Induction and deduction
Network Coding

- Linear combinations of packets

\[
\begin{align*}
q_1 &= \alpha_{1,1} p_1 + \alpha_{1,2} p_2 + \alpha_{1,3} p_3 \\
q_2 &= \alpha_{2,1} p_1 + \alpha_{2,2} p_2 + \alpha_{2,3} p_3 \\
\vdots \\
q_k &= \alpha_{k,1} p_1 + \alpha_{k,2} p_2 + \alpha_{k,3} p_3
\end{align*}
\]

- **Trade-off:** security and fault tolerance *(ICCCN 2017)*
  - Active vs. passive: Byzantine vs. eavesdropping
  - More transmission: more robust, but more vulnerable
  - Low-complexity cryptography: encrypts coefficients only

- **Inter-layer coding:** efficiency/reliability trade-off *(ToN 2016)*

\[
\begin{align*}
\alpha_{1,1} p_1 + \alpha_{1,2} p_2 + \alpha_{1,3} p_3 &= \alpha_{1,1} p_1 \\
\alpha_{2,1} p_1 + \alpha_{2,2} p_2 + \alpha_{2,3} p_3 &= \alpha_{2,1} p_1 + \alpha_{2,2} p_2 \\
\alpha_{3,1} p_1 + \alpha_{3,2} p_2 + \alpha_{3,3} p_3 &= \alpha_{3,1} p_1 + \alpha_{3,2} p_2 + \alpha_{3,3} p_3
\end{align*}
\]
Key Generation

- **Random signals (which signal?)**
  - Shaking trajectory (ShakeMe, IUCC 2015)
  - Gait (Walkie-Talkie, IPSN 2016)
  - Magnetic signals (MagParing, TIFS 2016)
  - Electromyography (EMG-KEY, Sensys 2016)
  - Ambient wireless signals (ProxiMate, Mobisys 2011)
  - Channel state information (TDS, CCS 2016)

- **Quantization**
  - Performance and security trade-offs
  - Usability

<table>
<thead>
<tr>
<th>ProxiMate</th>
<th>ShakeMe</th>
<th>Walkie-Talkie</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.8</td>
<td>8</td>
<td>70</td>
</tr>
</tbody>
</table>

Bit rate (bit/sec)

- EMG-KEY: 5.51
- MagParing: 28.4
- TDS: 100
Near-Optimal ILP (Trustcom 2017)
Backbone Local Marking

Marking a **backbone locally** in MANETs

- A node is a backbone node if it has two unconnected neighbors
- Non-backbone node: if its neighbor set is covered by several connected and higher priority nodes