TAIRO: Trust-aware Automatic Incremental Routing for Oppnets

Joseph W. Baird (Adviser: Dr. Leszek T. Lilien)
Department of Computer Science

1. Overview

- *Opportunistic Resource Utilization Networks* (*Oppnets*) represent an emerging technology in computer networking [1,2]. They are specialized ad hoc computer networks that require a specialized routing protocol developed specifically for them.
  - *Routing protocols* select the *paths* (sequences of links *and nodes*) over which network traffic travels. There are dozens of computer network routing protocols. Some choose the shortest path between source and destination, others look for the fastest path, etc.
- Trust-aware routing protocols are also an emerging field in computer networks and computer security.
  - *A trust-aware routing protocol* looks for paths that are trustworthy.
    - A *trustworthy path* means that the intermediate nodes (between a source and a destination) are expected to be forwarding messages very reliably.
  - A *trustworthy network node* has the requisite *software* to handle routing duties, powerful enough *hardware* to meet the network's transmission requirements, sufficient *battery power* to receive and forward messages, and—most importantly--the required *reputation* for performing without failure or malevolence.
    - A node that is known to be exposed to the potential danger of attacks from malicious insider or outsider nodes is less trustworthy than a node with no such exposure.
- *Automatic Incremental Routing (AIR)* is a novel scheme for designing network routing protocols. [3]
  - Most routing protocols use some mechanism to discover an *entire node-to-node path* whenever a node transmits a message.
    - This requires the transmission of a flood of *route discovery messages*—before the actual data message can be sent—resulting in large transmission overhead.
    - AIR assigns a *prefix label* to each network node in such a way that transmissions can be routed from source node to destination node in small local increments, without the need to discover the entire path all at once. [3]
    - These small, local "mini-paths" are automatic, without a need to first send any route discovery messages.
      - This greatly reduces network transmission overhead. [3]
- Trust Awareness and Automatic Incremental Routing should be well-suited to Oppnets, due to the central purpose of Oppnets, and due to the way Oppnets grow.
- We believe that TAIRO can provide trustworthy routing for Oppnets.

2. Background: Oppnets – An Enabling Technology for Pervasive Computing

- *Basic Oppnet idea*: Serve applications via specialized ad hoc networks based on the idea of gaining "*helpers*" that can provide additional resources when the application requires or can benefit from such resources.
  - Helpers are *recruited* from among external devices, networks, computer systems, applications, etc. Helpers are *released* when no longer needed.
  - Two categories of helpers: pre-registered *reservists* (can be *ordered* to help), and ad hoc *volunteers* (have to be *asked* to help).
- A *Seed Oppnet* is a pre-designed network with a specific task to fulfill [1,2].
  - The Seed Oppnet searches for helpers that are able to help it with its tasks.
- After a Seed Oppnet finds and integrates helpers able to assist with the Oppnet's mission, it grows—in an ad hoc way—into an *Expanded Oppnet* [1,2].
  - Oppnets are designed to leverage *all* resources that the Oppnet nodes possess or can find.
    - This includes communication, computation, sensing, actuation, storage, etc. (cf. Fig.1).

References

[1] L. Lilien, Z.H. Kamal, V. Bhuse and A. Gupta, "Opportunistic Networks: The Concept and Research Challenges in Privacy and Security," *Proc. Intl. Workshop on Research Challenges in Security and Privacy for Mobile and Wireless Networks* (*WSPWN 2006*), Miami, Florida, March 2006, pp. 134-147.

[2] L. Lilien, A. Gupta, Z. Kamal, and Z. Yang, "Opportunistic Resource Utilization Networks—A New Paradigm for Specialized Ad Hoc Networks," Special Issue on Emerging Wireless Networks, *Computers & Electrical Engineering*, Elsevier, March 2010, pp. 328–340.

[3] J.J. Garcia-Luna-Aceves and D. Sampath, "Scalable Integrated Routing Using Prefix Lablels and Distributed Hash Tables for MANETs," *IEEE 6th Intl. Conf. on Mobile Ad Hoc and Sensor Systems (MASS 2009)*, Macau, China, pp. 188-198.

3. Problem Description

- Basic requirements for Oppnets:
  - A high level of security and service quality, including routing security and quality.
  - A specialized routing protocol optimized for Oppnets.
  - The addition of trust-awareness to Oppnet routing must not be burdensome for Oppnets by adding an unacceptable level of overhead.
    - For example, require nodes to retain trust information only about their immediate neighbors, rather than about all network nodes (thus reducing storage and computational overhead).
- Trust-awareness additions may include:
  - Modifying the composition of routing packets to include trust information and requirements.
  - Removing encryption requirements when the level of trust is high (thus decreasing computational overhead).
  - Assigning an entire network a security level that includes its trust-awareness (based on the purpose of the network).
  - Including a special, extra monitor node (or nodes) to keep track of trust information about the nodes (and, potentially, routes) found in the network.
- Hypothesis 1: Oppnets can be made more secure with a trust-aware routing protocol, if such use of trust-awareness will not overburden the Oppnet.
  - Trust-awareness will enhance the security and reliability of Oppnets in ways that can be measured.
    - These measurements can be compared to similar proposals for other types of networks.
- Hypothesis 2: Automatic Incremental Routing (AIR) can improve the performance of Oppnets by greatly reducing the need to flood the network with route discovery and other control messages.

4. Methodology

- Make an extensive study of known trust-aware protocols for general ad hoc computer networks, and create a *taxonomy* of these protocols.
- Devise mechanisms for a *distributed repository of trust information* about the nodes in the network.
  - This includes dynamically updated records of reputations, software configurations, hardware configurations, etc.
- Establish *default trust levels* for the various types of Oppnet nodes.
  - Types of Oppnet nodes: seed nodes, reservist nodes, volunteer nodes, and "lightweight" nodes (such as motion detectors).
- Modify AIR to meet the specific needs of Oppnets, from their initial creation to the way that they grow and add resources.
- Conduct *simulation experiments* for the designed versions of TAIRO.
- *Compare the performance* of TAIRO with the performance of other trust-aware routing protocols for non-Oppnets.

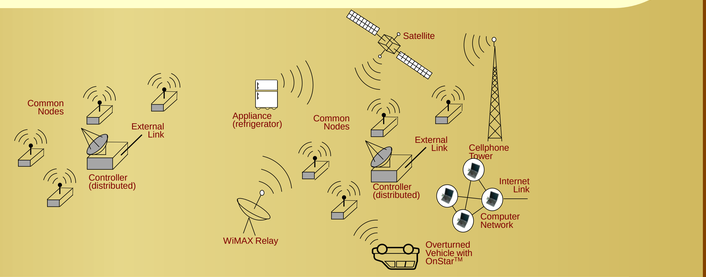

Figure 1. A Seed Oppnet (left) can grow into an Expanded Oppnet (right) [1,2].

5. Contributions

- Creation of a taxonomy of currently proposed trust-awareness enhancements will contribute to the theory and practice of ad hoc network routing.
- The creation of a routing protocol for Oppnets is an important step toward their implementation and deployment.
- TAIRO will greatly enhance the security and reliability of Oppnets, making their deployment more desirable.
- TAIRO extends previous theoretical work on AIR in general to its implementation in a specific type of a real-world network.
- Oppnets can assist, e.g., first-responders at disaster scenes, where secure and reliable communications are essential.
  - TAIRO will be especially valuable because Oppnets will encounter and communicate with potential helpers of unknown pedigree.

6. Status of Work and Future Work

6.1. Completed and In-progress Work

- Became familiar with current Oppnet theory.
- Finished a critical examination of the literature
  - Beginning to classify the various known trust-aware protocols.
  - Choosing which network routing performance metrics to use in judging TAIRO's operations.
- Mastered the fundamentals of AIR.
- Have begun rudimentary simulation programming.
  - Some decisions need to be made about the kinds of data to collect before continuing this work.

6.2. Planned Future Work

- Provide a taxonomy of proposed models for adding trust-awareness to general-purpose ad hoc computer network routing protocols.
- Design software simulations to test different versions of TAIRO.
  - Choose which of TAIRO's performance data to gather during the simulations.
    - Based on a review of the dozens of metrics in use in general-purpose computer networking.
  - Use mathematical modeling to gain a theoretical prediction of TAIRO's behavior.
- Simulate TAIRO and other trust-aware routing protocols for a variety of Oppnet topologies and categories.
  - The final composition of an Oppnet is unknown when the Seed Oppnet begins operations.
  - Oppnet nodes can be mobile and the network's topology can change dynamically, requiring the discovery of new routes.

6.3. Possible Future Extensions

(beyond the currently planned scope of this Ph.D. research)

- Adding additional encrypted transmissions in TAIRO to increase security; analyzing overhead.
- Using trust information maintained by TAIRO to help decide which candidate nodes are best suited for a particular, *non-routing* task.
- Investigating whether an Oppnet should take risks by accepting helpers with lower trust levels if they can provide highly desirable resources.
- Adding enhancements to TAIRO that would speed the repair of broken routes in the network.
  - A particularly vexing problem in ad hoc networks, where nodes join and leave the network at whim, and move in and out of range of each other at random.