Secure Content Centric Mobile Networks

M. Chuah, X. Xiong
Lehigh University

Abstract
New wireless technologies allow mobile users to have easy access to real time data, and stay connected with friends, colleagues, & business partners. However emerging applications are usually data-centric but existing IP oriented paradigms are not flexible enough to support this. To support emerging mobile applications, we are developing a next generation mobile network that supports mobile content centric networking features, namely (a) intentional named message delivery, (b) content-centric security, (c) push-pull based data disseminations.

In our new SECON network, users can send User Interest (UI) packets to Content Resolution Server (CRS) to request for content data (CD) packets associated with a particular URI. The UIs will be forwarded by the receiving CRS to other CRSes that know who will be publishing content packets related to that URI. The UIs can also have intentional-named destinations e.g. all CRSes within a certain geographical area. In addition content publishers can send content publish announcement (CPAs) to CRSes before they forward content data packets to these CRSes. We have a preliminary prototype that supports UI, CPA & CD features. We also support CPA aggregation feature. More features will be added in the near future.

Experiments

Secure Content Centric Mobile Networks

In the above diagram, we show the initial prototype of our content centric router.
• When data packets are received, the packet processing agent generates a packet received event to an external router daemon.
• The external router daemon will parse the packets to determine if the packet is meant for the node and/or needs to be forwarded. A resolver is consulted for forwarding packets with intentional named destination.
• Once determine the received packet should be processed by the node, the packet processing agent determines which manager should handle the packet e.g. CPA manager or UI manager. Each manager will extract information from the packet and update relevant tables.

In the above diagram, we show a few domains: ORBIT, Lehigh DTN, and DOME are infrastructureless wireless networks, PlanetLab is a wired IP-based testbed, XSM is a sensor network. We intend to deploy late binding routers and some mobile applications in each of these testbeds to demonstrate our intentional named message delivery feature. We will add security feature later on.

Our intentional named message delivery feature allows messages such as “secon:intent:role=students, university=lehigh, loc={Packard Lab, 100m})” to be delivered to all lehigh students that are currently located in a target region described as within 100m of Packard Lab (our CS building). Our current prototype is more efficient than CCNX in delivering contents.

Future Work
• Extend aggregation feature
• Design & Implement UI with keyword feature
• Design & Implement mobility support feature
• Evaluate emulation and testbed options
• Learn how to use DOME
• Add security features

Use of GENI Infrastructure

ORBIT/DOME
• Develop scripts that mimic nodes moving according to certain mobility models, e.g. Random Waypoint Group Mobility Model, Manhattanitain Mobility Model.
• Develop some sample applications that use intentional named message delivery
• Develop GUI for these applications.
• Deploy our prototypes on ORBIT & DOME
• Evaluate delivery performance.

Current and Proposed Publications

Acknowledgement:
We gratefully acknowledge NSF support for this work. We also thank I. Seskar for helping to answer questions about ORBIT exppt.