CERIAS

the center for education and research in information assurance and security

The MicroOppnet Testbed for Trust, Security, and Privacy Experiments in Heterogeneous Environments

VarunKrishna Kundoor,[1] Vikash Achutaramaiah,[1] Leszek Lilien,[1,2] Zille Huma Kamal,[1] and Ajay Gupta[1]

[1]The WiSe (Wireless Sensornets) Lab, Department of Computer Science, Western Michigan University [2]Affiliated with CERIAS

1. Introduction to Opportunistic Networks (Oppnets)

- The goal of *opportunistic networks* or *oppnets* is opportunistic leveraging of resources in possession of systems that are within oppnet's reach. It is achieved via integration of diverse communication, computation, sensing, storage and other resources [1]. We distinguish two basic types of opportunism in networks:
  - *Class 1 opportunism* — limited only to opportunistic use of communications.
  - *Class 2 opportunism* — when all kinds of resources, not just communication resources, are used opportunistically as needed by the oppnet.
- An oppnet starts its operation as a *seed*, a predesigned yet ad hoc (in terms of node locations) network. At an extreme, the seed can be a single node.
- The seed grows into an *expanded oppnet* by integrating helpers.
- A *helper* is an external system offering its resources or services to an oppnet. There are two categories of helpers: volunteers and reservists [2].
- *OVM* (*Oppnet Virtual Machine*) is a standard implementation framework for oppnets. OVM allows development of standard library routines and APIs for interoperability among all kinds of oppnet-based or oppnet-enabled systems.

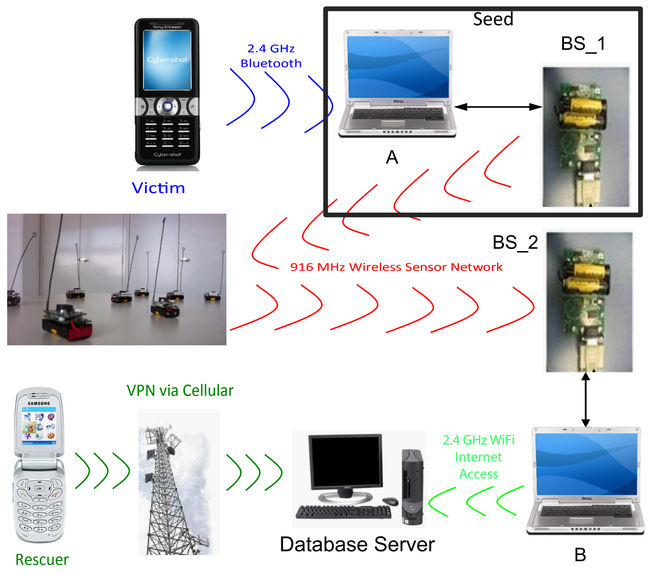

Figure 1. Structure of MicroOppnet v.2.3

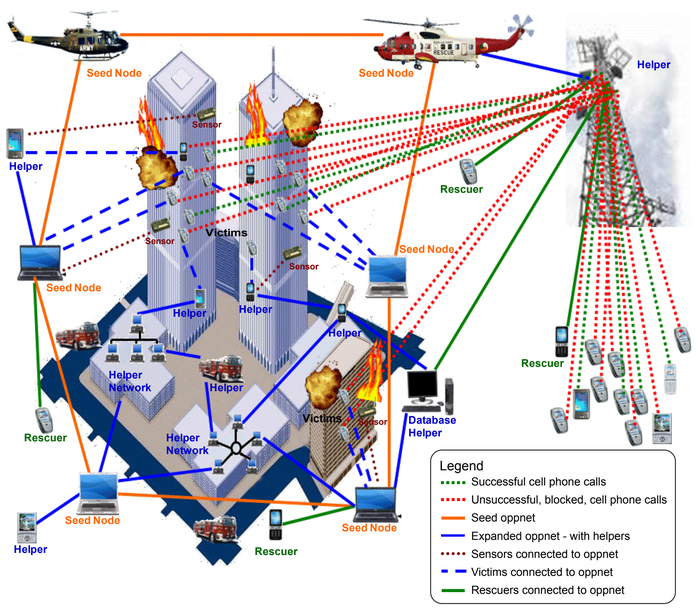

Figure 2. Oppnet emergency use scenario

2. Design of MicroOppnet v.2.3

- *MicroOppnet* is a small-scale testbed for oppnets [3].
- *MicroOppnet v.2.3* integrates Bluetooth, sensor networks, and wired and wireless Internet communication technologies.
- The seed oppnet for MicroOppnet v.2.3 consists of a laptop and a sensornet base station (cf. Fig. 1).
- The expanded oppnet adds the following components to the seed: a desktop, a laptop with an attached sensornet base station and many sensor motes, and two cell phones, with only one of them (labeled as "Rescuer") using cellular services.
- Seed can search for helpers within its Bluetooth range, or can just listen for signals from candidate helpers and victims.
- The MicroOppnet structure shown in Fig.1:
  - Victim can send a "Help" message to the seed (either directly or via any helper; only the former case is shown).
  - Base Station 1 (BS_1) can propagate the "Help" messages received by the seed to sensornet nodes. BS_1 can also command the sensornet to start sensing (e.g., taking temperature readings), and pass results to Base Station 2 (BS_2). Note that all sensornet nodes, except BS_1 but including BS_2, are helpers.
  - Sensornet nodes forward victims' messages and sensor data to BS_2.
  - Laptop B, to which BS_2 is attached, forwards data to Database Server, which is a helper.
  - Rescuers can query Database Server to retrieve the "Help" messages or temperature readings.
- Opportunistic communication realizes class 1 opportunism. Opportunistic sensing realizes class 2 opportunism.

3. MicroOppnet v.2.3 Implementation Details

Hardware:

- Sony Ericsson K550i & Samsung T209 cell phones
- Dell Inspiron 6400 laptop
- Kensington Bluetooth USB adapter 2.0
- Crossbow programming board and Mica2 Motes

Software and Services:

- ElectricBlue: JSR-82 Bluetooth stack for MS Windows
- Java 2 Micro Edition / Java Development Kit 1.5
- TinyOS for sensornet programming
- Cellular VPN service

4. Lessons Learnt

- Need to find devices, APIs and drivers that are compatible with each other.
- Free APIs for MS Windows are not easily available.
- In the future, some of the communication technologies, not available freely on MS Windows, will be implemented on Linux.

5. Experiments on Trust, Privacy & Security

- We have started work on a broad range of projects, which either already resulted in MicroOppnet experiments or will lead to such experiments. These projects include:
  - Authentication of helper candidates and oppnet nodes in oppnet environments.
  - Malevolent host masquerading as an oppnet member or as a helper.
  - Intrusion detection in oppnets.
  - Helper privacy and oppnet privacy.
  - Trust-based routing in oppnets, and in non-oppnet systems using oppnet-like helpers.
  - Using the Semantic Web for agent trust in oppnets.
  - Software agents' role in oppnet privacy & security solutions.
- MicroOppnet includes a variety of wireless subnetworks.
- Therefore, in addition to experiments in the heterogeneous MicroOppnet environment, this work includes privacy & security experiments in: mesh networks, WiMAX networks, sensornets, RFID networks and Software Defined Radio (SDR).

6. Emergency Use Scenario

- A fire starts in a large office building. Some workers or customers are unable to evacuate.
- Cellular network is overloaded, esp. due to thousands of calls made by people gathered outside. Only some calls succeed (green dotted lines), while many call attempts fail (red dotted lines). Many victims are among callers who are unable to call (red dotted lines originating in the towers).
- Rescuers deploy an oppnet seed (nodes connected by orange lines).
- The seed uses oppnet-enabled victim devices to discover victims, and develops communication among victim and helper nodes (blue broken lines). "Help" messages from victims are forwarded to Database Helper.
- Rescuers use "Help" messages stored in Database Helper to localize victims (green lines connecting rescuers to Database Helper, e.g., via oppnet or cellular services).
- Oppnet contacts all oppnet-enabled sensing nodes within the building & tells them to provide temperature readings (dark brown dotted lines). They are forwarded to Database Helper & stored there.
- Firefighters use the heat profile (produced from temperature readings) to find the best routes for rescuing people trapped in the towers.

7. Conclusions & Future Work

- Hardware availability should be the only limitation for other MicroOppnet implementations.
- MicroOppnet v.2.3 serves well as a testbed for pilot implementations of oppnet protocols & primitives.
- Extending the range of communication media by integrating IrDA, WiMAX, and RFID technologies.

References

[1] L. Lilien, Z. H. Kamal, V. Bhuse, and A. Gupta, "Opportunistic Networks: The Concept and Research Challenges in Privacy and Security," chapter in: *Mobile and Wireless Network Security and Privacy*, ed. by K. Makki *et al.*, Springer Science+Business Media, Norwell, MA, to appear ● [2] L. Lilien, A. Gupta, and Z. Yang, "Opportunistic Networks for Emergency Applications and Their Standard Implementation Framework," *Proc. 1st Intl. Workshop on Next Generation Networks for First Responders and Critical Infrastructure (NetCri07)*, New Orleans, LA, Apr. 2007 ● [3] Z. H. Kamal, A. Gupta, L. Lilien, and Z. Yang, "The MicroOppnet Tool for Collaborative Computing Experiments with Class 2 Opportunistic Networks," *Proc. 3rd Intl. Conf. on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2007)*, White Plains, NY, Nov. 2007

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center