

Opportunistic Sensor Networks (Oppnets)

Leszek Lilien, Zille H. Kamal, Ajay Gupta, Vijay Bhuse, and Ziji Yang, *Members, IEEE*

Index Terms—Sensor networks, opportunistic sensor networks, rescue and recovery, security, privacy.

We present Opportunistic Sensor Networks (oppnet), in which a set of nodes are deployed with the purpose of integrating nodes or systems in diverse communication media under one umbrella. This integrated medium will be the fundamental layer, upon which numerous applications can be built such as rescue and relief, emergency preparedness and response, to mention a few. To the best of our knowledge, we are the first to define and scrutinize this paradigm [1, 3].

Oppnets are a superset of Mobile Ad hoc Networks (MANET), which contain sensor networks. Traditional networks are deployed together with fixed, pre-defined network parameters, such as size, location, etc. We propose to deploy seed oppnet on the fly, where they will configure into an ad hoc network, however, after this 'set-up' the seed nodes are employed to detect the presence of nodes or systems in different communication media, such as Bluetooth, Wired Internet, WiFi, Radio, RFID, Satellite, etc.

These detected systems are then identified, classified and evaluated for their usefulness and reliability as candidates for joining the oppnet, after which potential candidates are invited to the oppnet. Candidates can accept or reject the invitation, on accepting the invitation candidate system is admitted into the oppnet. The resources of this helper system are then integrated with the oppnet and tasks can be offloaded to or distributed amongst these helpers. A human interactive and/or autonomous decentralized command center will preside over the workings of the oppnet throughout the life of the oppnet. When the goals of the oppnet have been realized, it is imperative to release helpers and restore them to the state that is closest to the state that we found them in, minimizing intrusiveness of helper. Figure 1, depicts these processes of the oppnet.

In such a manner, oppnets can be used as a bridge between disjoint communication media, and/or leverage various available services, and/or provide access to sensory data from diverse sensing systems that are already present in our environment.

Our goal is to take existing solutions in related areas and adapt them for oppnets. Growth in oppnets most closely resembles growth in Peer to Peer (P2P) systems, in particular unstructured, decentralized P2P systems like Gnutella [2]. The expansion of oppnets is analogous to the spread of malicious

instances of worms and viruses. Techniques for integration and management of heterogeneous nodes and devices in oppnets could trail after the techniques employed in grid-systems. One of our main goals is to take existing solutions and engineer them to achieve the goals of the oppnet.

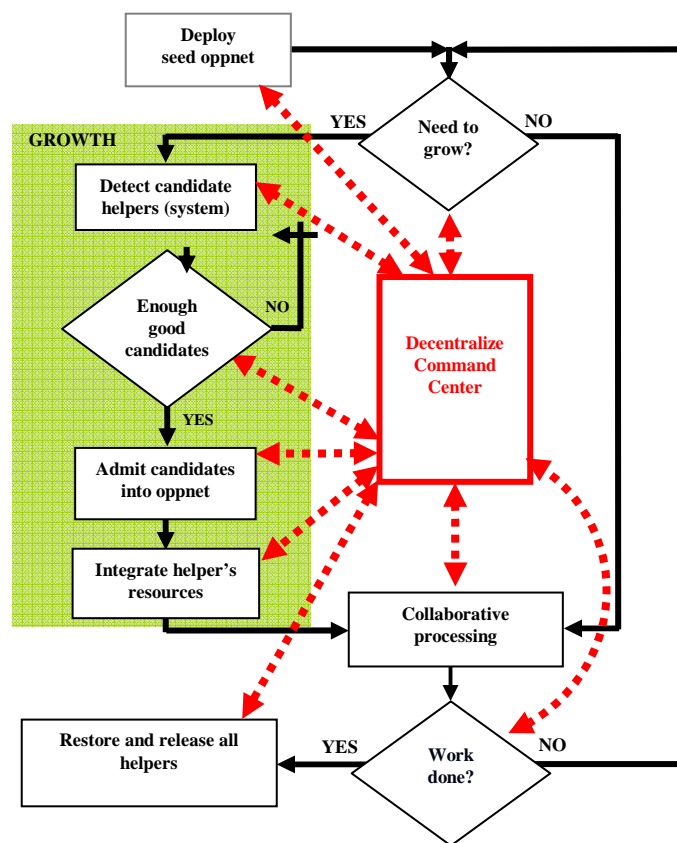


Fig. 1. Delineates and depicts the workings of an oppnet.

We will present the numerous research challenges involved in oppnets including initial solutions to some of them.

REFERENCE

- [1] L. Lilien, Z.H. Kamal, V. Bhuse, and A.Gupta, "Opportunistic Networks: The Concept and Research Challenges," *International Workshop on Research Challenges In Security and Privacy for Mobile and Wireless Networks (WSPWN 06)*.
- [2] R. Subramanian, and B. Goodman, "Peer-to-Peer Computing: The Evolution of a Disruptive Technology," Hershey, PA, USA: Idea Group Publishing, 2005.
- [3] B. Bhargava, L. Lilien, A. Rosenthal, and M. Winslett, PervasiveTrust," *IEEE Intelligent Systems*, vol. 19(5), Sep./Oct.2004, pp. 74-77.